

Master Thesis
Computer Science
Thesis no: MCS-2008:6
January 2008



Mobile payment with customer controlled connection

- Can it be constructed to be safe enough?

Samuel Ivarsson

Department of
Systems and Software Engineering
School of Engineering
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

This thesis is submitted to the Department of Systems and Software Engineering, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:

Author(s):

Samuel Ivarsson

E-mail: samuel.ivarsson@gmail.com

External advisor(s):

Johan Persbeck

Cybercomgroup Sweden South

Address: Campus Gräsvik 1, 37141 Karlskrona

University advisor(s):

Martin Boldt

The Department of Systems and Software Engineering

Department of
Systems and Software Engineering
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

Internet : www.bth.se/tek
Phone : +46 457 38 50 00
Fax : + 46 457 102 45

ABSTRACT

The mobile commerce has given birth to many mobile payment systems and this thesis covers the security of a theoretical system where the communication is handled by the customer. There are many technologies that can be used when implementing such a system, each with different strengths and weaknesses. The system designed in this project was constructed for micropayments in vending machines that has no connection to the vendor except for the connection supplied by the customer. The design was then used for analyzing the threats against the designed system and comparing it to an identical system where the connection is supplied by the seller in order to find out the effects on security when changing the communication channel. The comparison shows that even though the designed system is more vulnerable, it is not a major difference and with low value payments, the mobile payment system can depend on the connection supplied by the user. The main advantages to security with this method is the protection against Denial of Service attacks and the protection against mass identity thefts as authentication is no longer done on the machine.

Keywords: Mobile, payment, security

CONTENTS

ABSTRACT.....	1
1 INTRODUCTION.....	4
1.1 ABBREVIATIONS.....	4
2 BACKGROUND.....	5
2.1 DEFINITION.....	5
2.2 SIMILAR SYSTEMS.....	5
2.3 DESIGN CONSIDERATIONS.....	6
2.4 TRUST.....	8
3 PROBLEM DEFINITION.....	9
3.1 MOTIVATION FOR THE PROJECT.....	9
4 METHODOLOGY.....	10
4.1 QUESTIONS.....	10
4.2 VALIDITY.....	11
5 GENERAL SYSTEM DESCRIPTION.....	12
6 SECURITY ASPECTS.....	14
7 THREAT ANALYSIS.....	16
7.1 METHOD.....	16
7.2 ANALYSIS.....	16
7.2.1 <i>Assets</i>	16
7.2.2 <i>Environmental threats</i>	16
7.2.3 <i>Deliberate Human Threats</i>	18
7.2.4 <i>Unintentional Human Threats</i>	23
8 TECHNOLOGIES.....	26
8.1 PAYMENT METHODS.....	26
8.2 COMMUNICATION METHODS.....	27
8.3 TRANSFER METHODS.....	28
8.4 TRANSFER DATA.....	30
8.5 SECURITY ASPECTS.....	31
8.6 MAINTENANCE.....	32
9 SYSTEM CHOICE.....	33
9.1 ANALYSED SYSTEM.....	33
9.2 REFERENCE SYSTEM.....	34
10 COMPARATIVE THREAT ANALYSIS.....	35
10.1 INTRODUCTION.....	35
10.1.1 <i>Scales</i>	35
10.1.2 <i>Goals</i>	35
10.2 COMPARED SYSTEMS.....	36
10.3 ATTACK TREES.....	36
10.3.1 <i>Aquire item(s)</i>	36
10.3.2 <i>Small scale privacy attack</i>	41
10.3.3 <i>Large scale privacy attack</i>	42
10.3.4 <i>Sabotage of a machine</i>	42
10.3.5 <i>Sabotage of transaction server</i>	44
10.3.6 <i>Sabotage the service for a single customer</i>	46
10.3.7 <i>Sabotage the supply service</i>	47

10.4 ATTACK TREE COMPARISON.....	48
11 DISCUSSION.....	49
11.1 AUTHENTICATION.....	49
11.2 AUTHORIZATION.....	49
11.3 AVAILABILITY.....	49
11.4 CONFIDENTIALITY.....	50
11.5 INTEGRITY.....	51
11.6 NON-REPUDIATION.....	51
11.7 PRIVACY.....	51
11.8 RELIABILITY.....	52
11.9 ADVANTAGES OF CONSTRUCTED SYSTEM.....	53
11.10 DISADVANTAGES OF CONSTRUCTED SYSTEM.....	53
11.11 EFFECTS OF COMBINING THE TWO SYSTEMS.....	53
11.12 SUMMARY.....	54
12 CONCLUSION.....	56
13 FURTHER WORK.....	57
14 REFERENCES.....	58

1 INTRODUCTION

The thesis concerns the security of mobile payment systems where the traffic only goes through the connection supplied by the customer. The purpose of using only this connection is to eliminate the need for, for example, a vending machine to be connected to an online payment system. This would make it possible to reduce the amount of cash that flows through the machine in comparison to an ordinary machine without electronic payment, while still maintaining the same sell rate and at a minimal investment cost. It would further make it possible for the seller to receive messages from the machines, such as problems, shortages and so on, thereby making it possible to optimize the supply route. As the need for cash decreases in the society, less people have cash at hand for the vending machine and a mobile payment system might be the solution to maintain sales at the same level. The purpose of this work is to study the possible threats by analyzing the threats to such a payment system in theory, create a system specification that takes these threats in to considerations and analyze the remaining threats. In order for mobile payment systems to be publicly recognized and used by the broader mass they need to be secure and safe to use.

1.1 Abbreviations

CPU – Central Processing Unit
GPRS – General Packet Radio Service
IDS – Intrusion Detection System
MSP – Mobile Service Provider
PKI – Public Key Infrastructure
SMS – Short Messaging Service
USSD – Unstructured Supplementary Service Data
WAP – Wireless Application Protocol

2 BACKGROUND

This chapter covers the definitions used in mobile payments, examples of similar systems and design considerations when designing a new mobile payment system. It also covers the role of trust in mobile business.

2.1 Definition

There have been quite a few attempts to categorize different types of mobile payment systems. Dennis Abrazhevich covers classifications and characteristics of payment systems, where the first category is whether the actual money is token based or an account mechanism, also covered in “Study of Mobile Payments System”[7][23]. Token based payment is not within the scope of this thesis as the requested payment system shall have a connection through the buyer’s mobile phone and has very different security aspects. Therefore tokens were never considered as a solution, although some research was made on the subject to find useful information that might be transferable to this design. The article also makes a difference between payment systems and mediating systems, where payment systems are when the seller settles the payment and mediating systems are when a third part handles the payment between the seller and the buyer. An example of a good mediating system is PayPal, where any users of the system can transfer money between them. The purpose of this is that as mediating system it would have a greater chance of being used in a wide array of situation and therefore attract a larger group of users.

Payment systems can also be categorized in the time aspects of the payment, if the payment is real time, pre-paid or post-paid [23]. Another classification is the payment medium, if it is paid by account/credit card or by phone bill [23]. As the designed system is aiming for the widest possible use and the payment by phone bill requires all MSPs to be a part of the system, the most supported method is to use account payment.

2.2 Similar systems

Mobile payment has been tried in many forms already, for example the Dial-a-coke system in Finland, which was developed by Coca-cola Drink and Sonera. It began as a project for connecting the vending machines to the distributor in order to keep track of machines running low on supplies. From that project grew the Dial-a-coke system, where the users call the vending machine to buy their soda. A disadvantage with this technology is the need for each vending machine to be connected with a phone line which is a large investment and raises the maintenance cost with the cost of the connection. That investment might however lead to saving money by optimizing supply routes. Already in the middle of year 2000, the Coca Cola Company had 65,000 machines online [25].

As that technology is based on the customers having a cellular with them at the time of the purchase they already have one connection from the customer and the system designed in this thesis relies entirely on this connection. The only thing needed is verification to the machine that the buyer has paid for the item; this thesis proves that this does not need a separate connection.

Another project that is very similar to the one covered in this thesis was carried out in Canada in 2004[3]. There the authors constructed a payment system without a permanent connection to the vending machine that uses infrared communication between the customer and the client. This idea was based on the calculation that 18% of the total amount of cellular phones had an IR-module in 2003 and that amount grows by 15-20% annually. They also have a complementary mode to the system where the user can type in the codes needed for the purchase. The communication then goes through the customers mobile to a back-end server that handles the information by sending payment information to the billing system and vending machine information to the vending operator site as shown in *Figure 1*. This system

has the key features used in the solution created but there is very little information about the system specifications available and the security aspects of the system has only briefly been covered. Therefore, this system has not been used in the construction of the threat analysis; instead a new system was created that resulted in a very similar system to this Canadian system with a few major differences and a lot more detail in order to analyse the threats against the system.

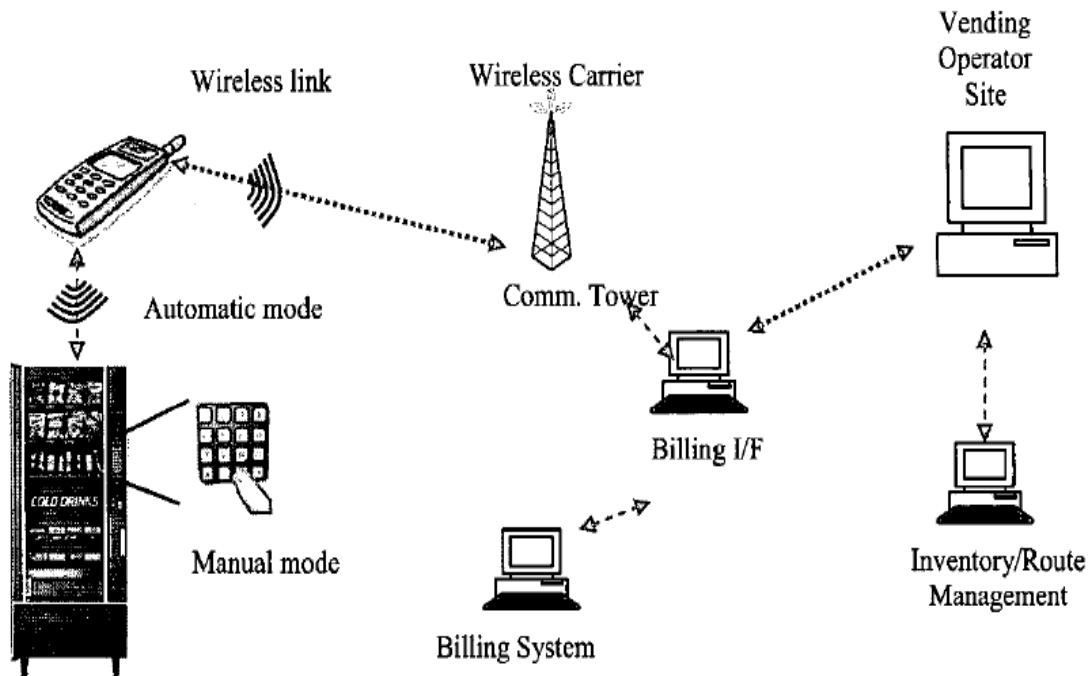


Figure 1: A payment system developed in Canada, 2004.

Other than this system, there is no other system to be found that uses this method for communication, resulting in a rather short background in regards to similar systems. The only mobile payment systems found not using a connection supplied by the seller uses a personal token as digital cash and does not relate in any real way to this thesis.

2.3 Design considerations

This section covers experience drawn from other mobile payment systems that should be taken in to consideration when creating a new one.

There are a few issues that can be considered as challenges to this system, as the aspect that a mobile payment system should be supported by many hardware platforms, such as cellulars, PDAs and laptops in order to be flexible and useful in a wider array of situations [8].

That article also brings up a few very important inhibitors on mobile commerce that has to be avoided such as high transaction cost; the MSP might charge too much for the traffic to make the purchase profitable in comparison to other payment methods, and inconvenience; the new payment method might be too inconvenient to be useful by the majority. Other issues are payment fraud; if it is possible to make money by not doing as expected or allowed it will probably be used to acquire something without paying, and merchant fraud; the delivery of purchased item/service might not be guaranteed. Unfamiliarity with e-commerce can also affect the payment system as both business and financial institutions lack the needed knowledge about mobile commerce and are uncertain of the cash flows. In that article they chose to solve some of these issues by using PKI.

Another issue is the certain characteristics of mobile devices, the size of the display, input devices, memory and CPU processing power, bandwidth capacity and the supported operating systems [19]. That article also brings up the advantages and disadvantages of mobile commerce, where the advantages are for example ubiquity; the user can use mobile commerce any where, any time. Localisation, that the user can be localised by the network operator and convenience, where the size and weight of mobile devices makes it possible to carry them constantly are other examples of advantages. Also personalisation is mentioned, as mobile devices are rarely shared between users, it can be used for personalised commercial to each customer.

Among the disadvantages mentioned in the article are display size, input devices, inadequate hardware and the limitations mentioned above. The very size of the mobile devices also makes them prone to theft which is a big problem, especially as they often contain personal valuable information for the user.

By researching other payment systems, some more or less common flaws were found that might have contributed to the small success of many systems. The most critical flaws that were found were the following four. To narrow niche, the technology was only used for one thing, this made the usage limited and the breakthrough never came. The payment system has to be usable in a number of daily situations, like parking your car, buying your soda, getting the newspaper or taking the buss, not just one of these situations. Secondly, the system might be too costly per payment. The cost for a credit check for one payment might cost as much as 10 cents [10]. For a can of soda this would represent somewhere around 5-10% of the total amount which cuts rather deep in the profit. The third flaw found was that the investment in electronic payment cost too much, for example, the payment system requires a link to the vending machine and the cost for this was too high to warrant the upgrade. The fourth and last flaw was the security issues where some systems for example allowed customers to spend their money more than once.

The research of prior systems has resulted in a list of valuable advantages of different mobile payment systems and the design in this thesis has been done trying to include the advantages in each solution while still avoiding the problems found in the studied systems. The Canadian article on offline vending machines mentioned the value of feedback from the vending machines to the vending company in order to optimize the supply route [3]. This is covered in detail in another article by the same authors, with simulations on the effect of feedback information and concludes that there can be a huge saving in supply costs when implementing this sort of systems [4].

Amir Herzberg in his article from 2003 brings up another benefit of mobile payments where the user can easily check the balance of the account and logs of previous purchases [9]. For this to be useful, the users must be able to use this technology in every day situations, like the grocery store, the gas station or the shopping mall. In order to make a mobile payment system more profitable, it should be designed to support as many different markets as possible, both to split costs on the common parts and to make the users see that it is usable in many situations.

In Norway there was a survey regarding the thoughts on mobile payment and one of the questions asked was "What do you think would make mobile payment services easier to use?"[12]. The most pressed upon point here was "Omnipresence, it must be accepted by many points of service", this answer was made by almost 70 percent of the survey group. Other aspects that more than 50 percent of the group thought would make it easier was "Better feedback, in terms of getting a better receipt" and "Improved user interfaces(easier to use)". These answers has been a foundation for the design of the payment system in this thesis, it should have a easy and familiar interface, provide easy access to an overview of previous transactions and above all, be usable in many different everyday situations.

As seen in the article “Offline Micropayments without Trusted Hardware”, risk management can be used to help reduce risks where the technology lacks a cost effective security defence [10]. In the article it was used on an electronic cash system but it is an important aspect to remember on this system also. An example of the use is to limit the number of times the device can be used for different tasks, e.g. you might only be able to spend 200 SEK on sodas on one day.

2.4 Trust

Trust in electronic commerce can be defined as a belief in the system characteristics, specifically belief in the competence, dependability and security of the system, under conditions of risk [11] Trust plays an important role in the success of electronic commerce and might be a critical issue in regards to the success or failure of a business [20]. Srinivasan describes many different views on trust and points at five key factors used to enhance transaction trust that should be considered when designing a new e-commerce system. Three of these can be applied to the kind of system designed in this thesis. The first factor is easy access to description of products and services; this could easily be placed on the physical machines but could also be made electronically with a web browser in the mobile device belonging to the customer. The second factor is the ease of placing orders; this should be made as easy as possible for the customer. The third factor is order confirmation, the customer should be allowed to view the order and verify that it is correct before approving it. The last two factors play an important role and should be incorporated in the technical specifications.

3 PROBLEM DEFINITION

The market for mobile payment systems is still searching for better ways of handling small value payments, so called micropayments, as used in vending machines. The benefits of having an electronic connection of some kind is apparent, the machines can instantly report the need for repairs or more supplies. Most current systems require a permanent connection to each machine, leaving the system dependant on the connections to the machines. The server handling the service can be protected against denial of service attacks but it would not be cost effective to protect each machine and an attacker could attack each machine separately from the Internet if they all have their own connection. The connection might also fail by unintentional reasons and the machine would then be unusable for mobile payments until this has been repaired.

A security issue that is addressed by this project is the issue of identity theft that otherwise can be accomplished by monitoring the equipment on the machines in order to copy the authentication information inserted. The most common identification tokens are credit cards that can be used in a wide array of situations to pay for items using the personal identification number associated with the card and that should be known only to the user. The use of credit cards as a payment medium makes mobile payment systems on vending machines very susceptible to attacks as these machines often are unmonitored and can be modified with information theft equipment without the suppliers knowledge, resulting in the theft of payment information for all cards used in the machine during the attack. Therefore, it should be possible and preferable to perform the authentication without making it accessible to an attacker monitoring the machine.

3.1 Motivation for the project

A possible mobile payment method has been proposed by the industry as a system where the connection is no longer supplied by the seller but by the customer. Using this system as a backup would make purchases less dependant on the permanent connection, keeping the service online even if the connection to the machine is interrupted for any reasons. This sort of system has been briefly covered in a Canadian study in 2004 where it was proposed as a primary system for mobile payments and did not cover much on the security aspects. In order to evaluate the method, the threats against such a system must be discovered and analyzed. This thesis aims at finding the threats specific to this method by comparing it to the common method where the seller supplies the connection. Should the method be considered as a better method than the common, it might result in more efficient mobile payment systems that can be used in a wider array of situations as they no longer require their own connection and could easily be installed on existing systems. At the very least, the result of this project should be usable as a base or a reference for any future threat analysis against mobile payment systems, something that the scientific papers is seriously lacking at the current date.

4 METHODOLOGY

This project was conducted as a literature study for setting the theoretical foundation and was then proceeded as explorative case study, where a system was constructed, threat analysed and compared to a reference system[6][16]. It began as a literature study of similar systems in order to construct a new system based on previous research. In this study, many similar systems were examined in order to find the good and bad qualities in other systems in order to construct a system that could be as usable as possible and take mobile payments one step further. The literature study also included finding and analyzing threats against mobile payment systems, preferably those usable in vending machines. Sadly, the publically available material on the threats against mobile payment systems is scarce and this emphasizes the need for this kind of studies.

After finishing the literature study, the the project proceeded as a qualitative case study and a new system was constructed where the seller does not supply the connection but relies on the customer[6]. The constructed system has great similarities to the system constructed by Azami and Tanabian but as their paper does not contain much details about the system, a new system was created together with a reference system. As no threat analysis could be found against their or similar systems, this case study was done in an explorative way and was concluded by a comparative study of the constructed system and the reference system, resulting in a comparison of threats against these two systems and a conclusion on how the threats are affected if the systems were to be combined[16].

4.1 Questions

The topic was chosen in agreement with Cybercomgroup in Karlskrona and as mentioned, the literature study showed that little has been written on the threats against mobile systems and no information on threats against systems where the customer's connection is used. There has been quite some work on mobile payment systems in general although very little with a dedicated focus on security. This led to the first question:

1. How can the connection be shifted from the seller to the user in a mobile payment system while still maintaining the same level of security?

In order to answer this much research was put into finding similar systems and any security aspects covered in these articles. In order to demonstrate how this can be done, a theoretical system has been constructed in the process of this project to test theories against. In order to be able to evaluate if the system is reasonably secure, the threats against the system has to be analysed. This led to the second question:

2. What are the threats against a mobile payment system where all communication is handled by the client?

In order to answer this, a threat analysis has been constructed against the theoretical system and against a theoretical reference system that operates in the same way but the connection is provided by the system instead of the customer. In order to not get too theoretical and make it possible to actually implement the system, the objective was set to make the system easy to use and construct. This led to the last question:

3. How can such a system be constructed to be secure enough while still being easy to use and cost effective?

A short description of the flow of the project:

The foundation was laid by doing a literature study of mobile payment systems, both systems described in research papers and systems that are used in the market at present. Based on the results from this, a general description of the proposed system was created in order to evaluate the threats against this sort of systems. The general description was made with the purpose of using the mobile payment systems on vending machines. With this in mind, the general threat analysis was done, resulting in a list of variables to consider when designing the system and based on this a system specification was created to make a complete threat analysis on. When the system had been designed, it was analysed using attack trees, focusing on a number of goals to accomplish. The same was done for a reference system where the communication is handled the traditional way in order to compare the two methods. The project finishes with a discussion, comparing the two methods in regards to the eight security aspects found and stated in chapter 6.

4.2 Validity

In regards to the validity of the study, this is highly dependant on the knowledge and expertise of the author(s) as is the case with all risk and threat analysis. The threats on the systems has been found by using the result from the litterature study, combined with the knowledge of the author, supported by articles on the different threats. As no concrete threat analysis could be found on mobile payment systems, this was done in an explorative way and using material from different areas of information security to find new threats to the system.

5 GENERAL SYSTEM DESCRIPTION

In this part there will be a brief overview of how a payment system could be designed to pass all the communication through the customer's mobile connection. It will only describe the possible communication flow in such a system using existing technologies and is left unspecific with purpose in order to not reveal any details about the specific system developed for Cybercomgroup, Karlskrona, available in Appendix A for authorized viewers.

In a traditional e-commerce system the communication would go from both the seller and the buyer to the payment authority to confirm the deal. The seller sends payment information to the buyer that contacts the payment authority and transfers the money. Then the bank informs the seller that the buyer has transferred money to the seller. The reason for this is that both parties should be secured by the payment authority that the deal was made correctly and does not have trust the other in order to make the deal. In this proposed system the trust is moved from the payment authority to be dependant of each other, the buyer supplying the connection between the machine and the transaction server that is owned by the seller who then requests the transaction of money. The transaction server might be handled by the payment authority, the mobile service provider or a third party. The customer now has to trust that the transaction server will make a correct transfer and deliver the code needed to prove this to the machine and the machine has to trust that the user has not in any way tampered with the message in order to gain something not paid for.

The basic design used in this thesis is the one described in Picture 1 and can use different methods for the transfer of data between the machine and the customer and for the communication between the customer and the transaction server. The common factor between all varieties is the communication line in Picture 1.

Machine – The vending machine used to buy items from, not connected.

Customer – The person making the purchase using a mobile connection.

MSP – Mobile Service Provider, the company that supplies the customer with a mobile connection.

Transaction server – The server responsible for evaluation of the purchases might be the same company as MSP or a third party responsible for the service.

Payment authority – The authority responsible for transferring money from one account to another at the time of purchase. This might be the same company as MSP, the same party as responsible for the service or any financial institute that can make the transfers requested by the transaction server.

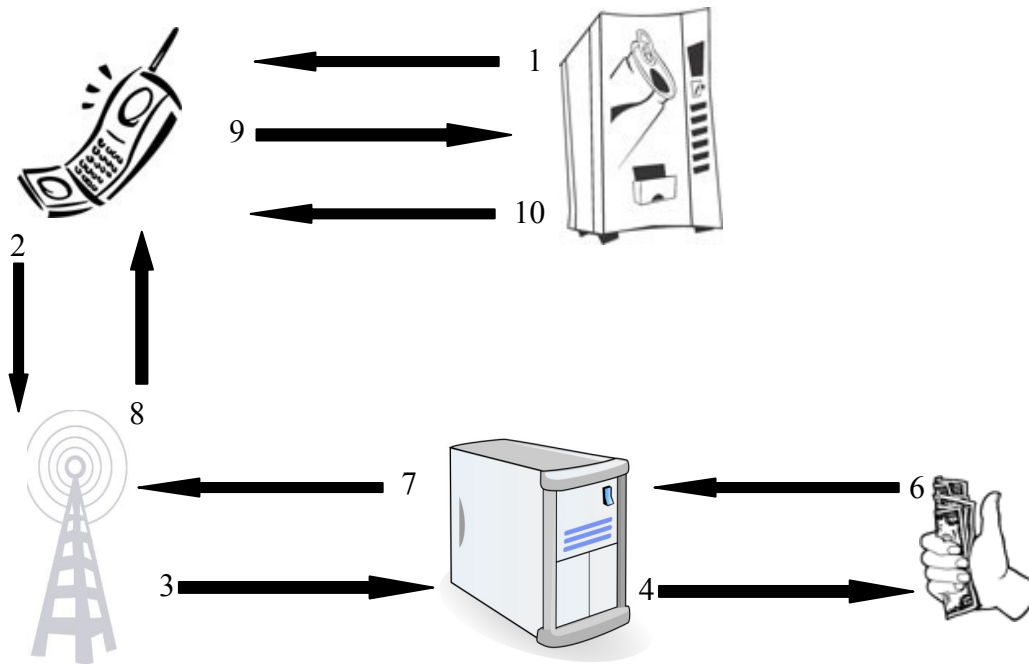


Figure 2, General design of communication in a mobile payment system

- Step 1: The customer gets message from the machine.
- Step 2: The customer forwards this message to the MSP.
- Step 3: The MSP forwards this message to the transaction server.
- Step 4: The transaction server decodes the message.
- Step 5: The transaction server sends a payment request to the payment authority.
- Step 6: The payment authority either approves or denies the payment request.
- Step 7: The transaction server sends a message back to the MSP.
- Step 8: The MSP forwards the message to the customer.
- Step 9: The customer forwards the message to the machine.
- Step 10: The machine checks the message and delivers the item if approved by transaction server.

6 SECURITY ASPECTS

The security challenges to mobile payment systems can be categorized into eight points [21] [2]. In alphabetical order, these are authentication, authorization, availability, confidentiality, integrity, non-repudiation, privacy and reliability. Privacy has not been covered in these articles but is an important aspect to consider in these times when more and more information is spread digitally. Authentication means that both the buyer and the seller should be able to prove to the other party that they are who they claim to be. This has to be valid through the entire chain of communication in order to stop man in the middle attacks.

By authorization it is implied that the purchase should only be possible if every condition for the purchase is met, e.g. there should be enough money on the buyers account and enough supplies in the vending machine. This is controlled at each end point in the communication flow; the machines only sell what is available and the transaction server checks with the payment authority before approving the purchase. Availability signifies the importance of the buyer and the seller being able to perform their business anywhere and at any time. The critical point here is the communication and it depends on the MSP to provide coverage for this. Naturally, the transaction server and the machines should always be online and waiting for a purchase, a threat to this might be a Denial of Service attack or simply a power outage.

Confidentiality specifies that nobody but the buyer and the seller should be able to read the communication. This relates strongly to privacy but can not totally protect the privacy of the customer as the communication still exists even though it is not readable. As the nature of mobile services is wireless, all the data is sent to anyone willing to listen and therefore one can not protect the existence of communication, one can only try to hide what has been said. In order to do this and hold the communication confidential, cryptography is needed. It is important to remember that cryptography might protect the present but that is no guarantee for the future, the keys used might be revealed or the encryption algorithm might be discovered to have a serious flaw. It is also difficult to use cryptography to hide the sender and the receiver even if the message itself is encrypted.

Integrity means that nobody but the buyer and the seller should be able to manipulate the communication. This is the other needed part of a defence against man in the middle attacks aside from authentication. If the integrity of each message can be guaranteed, no attacker can use an existing message to gain an advantage. With non-repudiation the users can be held responsible for the purchases made with the device, i.e. nobody else should be able to make purchases without the permission of the real user and the seller can claim the money from the customer. In this situation, with low cost items in a vending machine, risk management in combination with easier technology might be a reasonable solution to this instead of being over zealous.

Reliability is needed so that neither the buyer nor the seller loses any money if the payment system fails for any reason. The system should be constructed so that both sides get what they want at the same time. Besides that, the payment system should restart as soon as possible in order to prevent any further loss in transactions. In regards to privacy, any information saved should only be kept for completing current transfer and for making future purchases possible if the user has not expressed permission for the use of information in other purposes. This might however not be enough as the purchase information is broadcasted to anyone who listens and is therefore available to all. When cryptography is used, the information is hopefully not readable and the privacy given up can be kept to a minimum.

When reading the list of possible methods it is important to remember that some attacks are technically possible but most will probably not be worth the effort.

With this in mind, a general threat analysis against online vending machine was created according to method described by Peltier [14].

7 THREAT ANALYSIS

7.1 Method

The method used for the analysis greatly affects the results and a thorough study of different methods was done. By studying the pros and cons of qualitative and quantitative risk analysis it was decided to use a qualitative analysis which is more flexible and useful for the purpose of deciding the final specification of the system. There was also a lack of proper statistics for doing a quantitative study on such a theoretical system and impossible to calculate company based values, such as amount of customers and machines. It was however tested to send a survey over the qualitative study to 15 different vending companies in Sweden. Only one company answered on some of the questions and the study was not included in this thesis. After studying different qualitative methods for doing the analysis, it was decided to use the basic Risk Assessment described by Peltier with some changes [14]. The procedure consists of five steps in the book:

1. Asset Definition
2. Threat Identification
3. Determine Probability of occurrence
4. Prioritize Threats
5. Implementation of Countermeasures

As step 3 relied on the answers from the failed survey, the analysis was changed to a threat assessment instead of a risk assessment as the probability is no longer in the analysis. As step 4 depends on step 3, this was also struck from the analysis. The use of countermeasures in this early stage makes it easy to incorporate them to the designed system from the beginning and keep the costs as low as possible for the implemented controls.

7.2 Analysis

7.2.1 Assets

The following assets were found in the system:

Communication line – The communication line between the machines and the transaction server.

Reputation – The reputation of the company needed to acquire customers.

Physical machines – The physical machines.

Items – The items sold in the machines.

Resources – The money and staff of the company.

Encryption keys – The keys used for encryption of data between machine and transaction server.

Customer information – Information about the customers, such as personal information and history of purchases.

Payment information – Information about credit card numbers, payment history and other information regarding the customers payments.

Statistical information – Information about purchases, inventory and other impersonal information.

7.2.2 Environmental threats

Electrical disturbance

A short change in the power supply, either a voltage surge, voltage dip or a less than 30min power outage.

Cause:

A short power outage might be caused by a burned fuse, cut power for maintenance, a problem with the power supply to a wide area or by someone pulling the plug to the machine. A change in the power supply might be caused by other equipment on the same power supply or by an external interference such as lightning striking the building.

Effect:

This threat can result in three different effects. In the best case, the system continues to work as nothing happened when the interference is gone and nothing has to be mended. The second case is when the system reboots itself and all values are reset. This might destroy the payment protocol, depending on the implementation, as the machine has no free communication channel to the transaction server and has no way to re-synchronize without help from an external source. This might lead to customers buying codes that are no longer valid. In the worst case scenario, the electronic system can not reboot itself and has to be rebooted/repared by maintenance. In case one, it should not affect the system or sale in any mentionable way. In case two, it varies on the solution handling the communication and the implementation of the boot feature and might result in unmentionable loss in sale or a continuous loss until the problem is discovered. In the third case, the effect will be a continuous loss until the problem has been solved and the system is back online.

Control:

The effects show a need for a control in order to keep the system online, get the system back online automatically if it goes down and to notify when the system goes offline and does not automatically reboots. As this is likely to happen sometimes during the system lifetime, at least the reboot function should be considered as a requirement for the system and the two other optional.

Electrical interruption

A long power outage, longer than 30 minutes

Cause:

Might be caused by the same reason as a short power outage.

Effect:

A power outage should not result in any damage to the electronic system but the system will be offline for a longer period of time. This will result in a loss of sale during that time and if the system does not boot automatically on power on, there will be a loss of sale until the system is back online. This corresponds to the second case in the electrical interference threat. Should the machine also hold items sensitive to the loss of electricity, such as food needing to be cooled, it might also result in the loss of items in the machine.

Control:

Same controls as with electrical disturbance although the control to keep the system online during a longer power outage has to be modified if to support a longer period of time without external power supply. This might be better controlled by implementing the reboot function suggested in Electrical disturbance.

Hardware failure

A failure in the hardware of the machine resulting in a stopped system

Cause:

A part of the electronical system malfunctions because of bad quality, end of lifespan, an unintentional electrical current or the component is exposed to an environment it is not constructed for, such as high heat or high humidity.

Effect:

The system stops working in the intended way and makes the purchasing of items impossible for the time until the system has been repaired.

Control:

ESD protection of the sensitive area in the machine and using high quality electrical components. Placement of the system should be where it is as least likely to be exposed to environmental variables outside the specifications of the components in the system. Should the system stop working, the maintenance staff has to be informed in order to get the system back online as soon as possible. This should be taken into consideration when placing the machines and there should be a plan for getting information to the maintenance staff in case of interrupted service.

Telecommunications interruption

An interruption in the customer's mobile connection resulting in either loss of data or a failure to communicate or an error in the communication between the MSP and the transaction server

Cause:

This will naturally occur at places with bad or non-existing coverage from the MSP or might occur because of a MSP error or because of a user error, such as unpaid bills, bad battery or bad settings in the mobile device. An error in communication line between the MSP and the transaction server or either of the servers being unable to receive messages at the time of the transaction are possible reasons for interruptions in communication.

Effect:

This can result in incapability of making purchases until the problem is solved. Another problem that can occur is that purchases gets aborted anywhere in the transaction with a possible loss of data.

Control:

In order to minimize the chance of bad coverage, the machine should be placed at locations with good coverage from as many MSP as possible. If the customer can not make transactions because of user error or MSP problems, it can not be handled by the system but should be solved by the user with help from the MSP. In case of uncompleted transactions, this however must be handled by the system. This results in two different problems, the user has paid for an item not received and the machine is stuck at previous transaction that the transaction server regards as completed. The second problem must be handled in order to keep the system online and can be handled by the transaction server. In case of invalid message, check if it valid with a previous message and handle as a copy if it is the same sender and as a new transaction if it another sender. If it is a new transaction, mark the previous transaction as invalid and mark it for refund. This also covers the first problem. Obviously, both the MSP server and the transaction server should be as stable as possible to handle the transactions without any loss in traffic.

7.2.3 Deliberate Human Threats

Brute force code cracking

Trying all possible combinations until the correct one is found

Cause:

An attacker attempts to get a free item by trying all possible combinations in order to find one valid code.

Effect:

If there is no security at all and the code can be used again and again, the attacker can gain all items in the machine. If the code is only valid one time, the attacker will only get one item per valid code and be forced to start over when one valid code has been found. This might also sabotage the order of the transactions if the transactions have to come in a

particular order. If only one code is valid, the correct code will in average be found after having tried half of the possible combinations.

Control:

In order to make it harder to try all possible combinations, the transfer method should be locked for a period of time after each wrong entry. For each wrong entry, the transfer method freezes longer than the last time. To keep the usability and not creating a method for denial of service attacks, this lock function should be kept at a reasonable level, depending on the number of combinations and reset the lock function after a stopped attack. To make a found combination less useful, it should only be used once as a valid code. If the transactions have to come in a particular order, the transaction server will need to check ahead in the list of possible codes if the received message is invalid. This checking ahead should only be for a limited number of codes in order to reduce the risk of a customer having made a type error and buying an invalid code and corrupting the order of transactions even further. Depending on the method chosen for transferring the data, this might be very likely to happen on a daily basis and protection against this threat is necessary.

Emanation and eavesdropping

The readable emission from the mobile communications device and the machine and the also the communication between them

Cause:

The emission is emitted from all electronic devices when a change in current occurs. The range is dependant on how large the change in current is and how sensitive the equipment for reading the changes is. This threat also covers the messages broadcasted by sound, light and radio signals. All input and output, not just those broadcasted by radio, can be read by anyone with the appropriate equipment depending on the range.

Effect:

As every change can be read and therefore duplicated, it leaves the system open for replay attacks or man-in-the-middle attacks. It also makes it possible to study the system passively by setting up the eavesdropping equipment and record a large number of transfers in order to find a weak spot in the transaction protocol which could be exploited.

Control:

There are two ways to control this, either make it impossible to read the emissions or make it impossible to understand the emissions. However, this threat is highly unlikely to occur and if it were to occur, the only thing that would be worth the effort would be an exploit that will give free items to the attacker. A man in the middle attack would soon be discovered as the number of errors would be far greater than on any other machines if it used in any large degree and the attack is far to difficult to be used for just occasional theft of small value items. Replay attacks would be far more effective as this could be done without anyone reacting until maintenance staff observes that the machine inventory doesn't match the income and it would only need to record the transaction one time and then resend the information. To stop the threat of replay attacks, each transfer should be unique and sending the same data again should not result in any valid output. In order to stop a man-in-the-middle attack, there needs to be a system for authenticating the different operators in the system. To stop the attacker from understanding and breaking the system, the traffic from the embedded system within the machine to the transaction server needs to be encrypted end-to-end. Unless the attacker can read the information from the embedded system directly and figure out the key, this should make all transactions unreadable for the attacker. These controls should be considered as a requirement in order to keep the system working.

Vandalism

Physical destruction of the controls or the machine

Cause:

Someone exposes the machine for physical violence in order to destroy or to gain the contents of the machine.

Effect:

The machine partially or totally stops working until repaired. If the payment system is connected to a sensor for deliverance of the items, destruction might cause the payment system to believe that each transaction has been completed although no items are delivered or it might deny a new request in wait for a delivery that has already happened. It might cause the transfer method from the machine to the customer to stop working, and then no transactions can occur. If the transfer method from the customer to the machine stops working, then the customer can not get the item bought. However, this will probably result in a complaint and an alert of the problem.

Control:

Construct the machine so that the equipment can stand as much damage as is reasonable in regards to the possible losses. Put a phone number on the machine to call when broken or in case of failed transfers. Compare the transaction list from the machine with the list from the transaction server at regular intervals in order to find broken transactions to be refunded. These threats might be easier handled by risk acceptance, the control is probably more expensive than the effect.

Alteration of data

An intentional modification of data in an unintended way

Cause:

Modification of data on the transaction server in order to erase particular transactions in order to get a refund or to sabotage the system might be done by an insider or an outside hacker. Modification of data on the embedded system in the machine in order to know the encryption key beforehand using the same method as for updating the system if available.

Effect:

An invalid data input, modification or deletion on the transaction server might force the whole system to crash, resulting in a loss of income for the duration until repair. Depending on implementation, it might also erase all payment information currently unprocessed. In case of a valid modification of the transaction server, the owner will have no proof of the transactions and will be forced to refund the money for the deleted transactions. If the embedded system has a new encryption key, then the ordinary transactions will not work but the false ones supplied by the attacker will be approved by the machine.

Control:

Take precautions to stop an attacker from hacking the transaction server. Backup all information on the transaction server regularly and use checksums to verify that the data is correct. Have a redundant system so that another transaction server takes over the communication if the first one crashes. Save checksums separately and make them unavailable to the ordinary maintenance staff in order to discover any inside manipulation. Use logs and the list of checksums to find when and by whom transactions have been changed. In order to secure the embedded system, the update function has to be protected, both physically by a lock and by a code to update the system. In order to stay synchronized the transaction server should be updated first as it has more resources and can keep a new key while waiting for a signal from the machine to switch keys. As soon as the machine has been updated, the maintenance staff signals the transaction server that the current machine has been updated and will from now on use the new key. These are serious threats although not likely to occur and the controls should be required on the finished system.

Alteration of software

An intentional modification of the software in an unintended way

Cause:

An insider or outside hacker implementing a backdoor on the transaction server or on the embedded system. An insider or outsider hacking the transaction server and modifies the software to do unintended instructions other than a backdoor.

Effect:

The backdoor could be used for getting free items, either by using a backdoor in the machine that uses a special constant key to buy items without charge or by using a backdoor in the transaction server that does not charge any money from specified customers. The backdoor could also be used for gaining control over the transaction in order to manipulate or destroy the contents of the server. This could be used in order to blackmail the company, for example by threatening to destroy all information on the server or by using the software to encrypt all data on the server with a secret key that the company can buy for a specified amount of money. A backdoor could also be used for acquiring the personal data for the customers, such as phone number, credit card numbers and other information given to the company. Malicious software such as virus or worms released on the system could also make the system unavailable for purchases.

Control:

The transaction server software should be regularly monitored so it has not been changed since the last update and each change in the update should be monitored independently without rights to change the code to find any attempts to install a backdoor. Embedded systems in the machine should be hard coded in the system and it should not be able to update it by just downloading new software to it. It should not either be possible to download software from any of the systems in order to make it harder to manipulate the system. As a control method, the sold items should be checked against the inventory at regular intervals to find possible errors. In order to stop malicious software such as virus, an updated version of a good malware scanner should be run on the system, along with a correctly configured firewall and perhaps an IDS, which can also help find common errors in usage. These controls are common sense and should be implemented.

Intentional Disclosure

Unauthorized intentional release of sensitive information

Cause:

Release of the encryption keys for machines. Release of personal information about the customers. Release of payment information from the customers.

Effect:

Should the encryption keys be released to an attacker, the contents of the machine affected by this will be vulnerable until the key has been replaced. If personal information about the customers should be released to an attacker it would make an entry for a blackmail attack or for an attack on the credibility of the company. The information might also be sold further to a competing company. Release of payment information will result in the same effects but even more serious, the customers' money will be at risk and the company might be held liable. Release of purchase information, statistics and so on might be used for competition with the company for market shares.

Control:

Do not save more information than absolutely necessary. Store archive information offline with physical entrance control to that archive. Encrypt data on the system and log usage of information, restrict usage, storing and sending of sensitive information as much as possible. This threat is very diffuse and is almost impossible to totally control in a cost effective way and it might only be possible to accept the threat.

Sabotage

A deliberate action to disrupt company operations

Cause:

A sabotage of the physical machines, the transaction server or the communication line in order to stop or limit the usage of the system.

Effect:

A decreased or interrupted usage of the system resulting in a loss of income during the time of the sabotage or until repaired.

Control:

Same physical protection of machines as with vandalism. The communication line must be physically protected where it is possible and it must also be protected against attacks against the transaction server using the communication line, such as DOS attacks or malware attacks. The implementation of these controls is highly dependant on its cost efficiency and should be investigated further when the size of the system has been determined.

Theft

Unauthorized appropriation of anything of value in the system, such as data, software or hardware

Cause:

Theft of machine, items in the machine, part of the machine, theft of the transaction server or parts there of or theft of the mobile device for the customer.

Effect:

Theft of machine will result in loss of income for the period until replaced, cost of all items inside, the machine itself. Theft of items in the machine will result in loss of income until items are replaced, the cost of the items themselves and the cost to repair the machine if damaged in the theft. Theft of part of the machine might result in a loss of income until repaired and the cost of repair. It might also lead to the theft of items in the machine depending on part stolen. Theft of transaction server will result in loss of income until replaced, the cost of replacing all encryption keys if used and might result in blackmail or loss of reputation if the server contains sensitive information. The same effects will occur if the hard drive of the transaction server is stolen, otherwise there will only be a loss in income until the specified parts are replaced and the transaction server is back online. Theft of the mobile device for the customer might result in a number of unauthorized purchases and any payment information stored in the mobile device.

Control:

Physically construction of the machine to make it hard to steal the machine itself, any parts of it or the items inside it. The transaction server should be located in a room with restricted access and the contents on the hard drive should be encrypted by a key known only by a few trusted people and that is stored in memory while the server is running if the system is constructed so that sensitive information is stored on it. No payment information that could be used outside of the system should be stored on the mobile device, at least not without being encrypted with an algorithm considered safe with a key long enough. The information needed for the purchase should be more than just using the correct mobile device, it should also be combined with a secret key only known by the customer and those trusted by the customer. The use of a secret key should be considered a requirement for the system, all other controls can be considered optional depending on the cost efficiency.

Unauthorized use

An unauthorized use of the system

Cause:

An attacker spoofing another mobile device to buy items on the account of the other customer.

Effect:

An innocent customer gets charged for buying items never ordered, will probably be reported to the police with following legal consequences if the customer is not fully satisfied by the solution.

Control:

All transactions should require a secret code, known only by the owner of the mobile device and that holds the owner responsible for any purchases made with the mobile device with the correct code. Restrict the loss by setting a maximum amount that can be spent for a period of time. Log all information about transactions to and from the transaction server and keep these logs for a specified length of time. Investigate the logs from the transaction server to find where the order came from. If the order came from the MSP, request that the MSP investigate if the mobile device could have been spoofed at the specified time. Set a policy to either refund immediately with the option to charge the money later again or to wait with any refunds until the investigation is completed. The secret code and the policy for fraud should be considered as requirements for the solution.

Fraud

An unauthorized manipulation of the system in order to gain financially

Cause:

A customer calling and claiming the item or the code paid for never was delivered or even that it was never ordered in the first place, wanting a refund. Or a customer buying a large amount of items and then claiming the mobile device had been stolen and demanding a refund.

Effect:

A customer might be getting a free item as the system can not actually prove that the customer got the item.

Control:

Decide on a policy to either refund the money on complaint without waiting for verification or to wait with refunds until next maintenance control of the machine and then check if the code was ever entered in the machine and if possible, check if any items were delivered. In any case, keep track of reported malfunctions, if anyone sticks out in the statistics, it might be a fraud set in system in order to acquire free items. Also state in the customer terms whether the company will refund usage for a stolen mobile device. The most important control here should be deciding on a policy on how to act and determine further controls depending on the size of the problem.

7.2.4 Unintentional Human Threats

Alteration of data

An accidental modification of data on the system

Cause:

If using an update system for changing an encryption key this can result in the system being unsynchronized. Manual access to encryption keys might result in an accidental modification.

Effect:

If the system has been updated by maintenance staff, the system will be unsynchronized until the maintenance staff has informed both the transaction server and the embedded system to use the new key. An accidental modification to an encryption key might render the machine associated with it useless.

Control:

In order to stay synchronized the transaction server should be updated first as it has more resources and can keep a new key while waiting for a signal from the machine to switch

keys. As soon as the machine has been updated, the maintenance staff signals the transaction server that the current machine has been updated and will from now on use the new key. In order to control the manual modification of encryption key, it should only be able to easily create or delete encryption keys, not to view or modify them. Depending on the difficulty of creating valid fake messages, these controls might be necessary.

Alteration of software

An accidental modification of software on the system

Cause:

An accidental change in code, such as a type error that is accepted by the compiler.

Effect:

The effect might be software that behaves unpredictable or crashes seemingly at random.

Control:

Use software that keeps track of changes and highlights them. Use software that finds possible bugs. Let independent programmers review the code to find any possible errors. These controls should be implemented in some degree.

Bad design

The design does not cover all possible errors

Cause:

A design not covering all possible errors and opens for an attack because of insufficient knowledge by the designer.

Effect:

A flaw in the design might lead to an attack of some sort against the system if not discovered before launch of the system.

Control:

Use independent sources to verify the security and the validity of the design. Use personnel from different affected areas in the company to help evaluate the design and find flaws. These controls should be implemented in some degree, depending on cost efficiency.

Bad programming

The implementation does not follow the design perfectly or using insecure code

Cause:

Bad programming techniques, not following instructions accurately, insufficient instructions regarding the design.

Effect:

Might leave the system open for some sort of attack.

Control:

Use independent programmers to verify the accuracy of the code. Test the code before it is released. Inform the programmers to verify any unclear directives in the design with the designer. These controls should be implemented in some degree, depending on cost efficiency.

User error

User does not follow the complete buying sequence correctly

Cause:

User mistypes or aborts the purchase at any point without notifying the system.

Effect:

The effect might be input not handled by the system, resulting in unexpected actions and perhaps a crashed system. Other effects might be messages lost in transaction and an unsynchronized system.

Control:

Use a timeout function for inactive connections where the user has aborted the purchase. Handle unexpected input and inform the user that the input is invalid. Install a method for keeping the system synchronized. This is a situation that is highly likely to happen and should be controlled as a requirement on the system.

Unintentional disclosure

Unauthorized release of sensitive information

Cause:

Personnel releases sensitive information without knowing or unwilling.

Effect:

A release of sensitive information could seriously damage the reputation of the company with a possible loss in customers and if the sensitive information includes credit card numbers, it could also lead to a large theft from the customers for which the company might be held liable.

Control:

All personnel need to be aware of what information that may be released and to whom. An internal IDS might be useful here to alert when someone breaks the pattern and access information not within the normal working procedures. Both these controls should be required in the solution.

Comments to all threats

Almost all threats will have the effect of higher cost because of extra workload to fix the problem and to ensure it does not occur again.

8 TECHNOLOGIES

This section describes the different methods and technologies that could be used to implement the proposed system.

8.1 Payment methods

The method of payment can be either as an account or as a one-time payment. The difference between the two is the need for registration in order to create an account and the necessary account information that needs to be kept safe. In the case of accounts, the payment authority gets the information needed for charging the customer at the time of registration while a one-time payment has to send all information needed at the time of the transfer. The payments by account are either post-paid, pre-paid or real-time [23].

In post-paid, the payment is billed to the customer who gets an invoice on a regular basis. This has the advantage of not being in need of a connection to any external payment authority when making purchases, the transaction server just checks if the customer is cleared for further purchases and allows the purchase. By this follows the disadvantage with billing, there is no way of knowing if the customer has the money to pay for the bought item or how much effort it will take to get the payment. Another disadvantage of this is that the payment comes very late in comparison to the other methods.

With pre-paid, the payment is made in advance and the customer has a certain amount of credit available for payment. This has a clear advantage for the company supplying the service; they get the money beforehand and know exactly which customers that can buy items, without having to ask any external payment authority. It also has an advantage for the customers in regards to monitoring the purchases of these items, for example, a parent can insert a certain amount of money available to a child for monthly consumption of soda at school. However, the drawbacks of having to fill the account beforehand and the risk of the account being empty when needed might be too negative for the average consumer. There is also a risk of the company being liable if information about account balance is modified or lost.

With real-time, the payment is drawn from the customer's credit card in real-time. This could also be another third party payment authority, like PayPal or a gas station account. It has the advantages of instant payment, the company gets the money immediately after the purchase and the customer can only spend the money available on the account. The disadvantage is that it takes a little longer as an outside payment authority has to be contacted for each purchase in order to check if the purchase is valid and then for actually making the purchase. In security aspects, this variety also increases the threat to the company as the information has to be stored by the company in order to make the purchase and if it is in any way released to an outsider, the company might be held liable.

A solution worth mentioning here is when the MSP handles the payment. The payment is then charged to the customer's account used for the mobile communication. This is the system used by Sonera in Finland, the Dial-a-Coke service, where a customer calls the machine and buys the item. It is useful if the MSP supplies the whole service but might otherwise be a too costly service for a company handling the transaction server to buy. For the customer it has the effect that the bills from the MSP also include the purchases from vending machines. It also has the downside of service being bound to the MSP and is not usable by customers at other MSPs. However, when a payment has not been met, the MSP can threaten to shut down the customer's mobile connection which might serve as a big incentive to pay the requested money on time.

In the case of a one-time payment there is only the option of a credit card transfer; the information needed for the transfer is sent at the time of the order. It is however not bound to any account or mobile device and can be used anywhere and anytime. There are however severe limitations to this sort of payment, as there is much information to insert just to buy one soda and the information has to be well encrypted in order to be able to broadcast it to anyone listening. The transaction server then has to decrypt it and create an encrypted session with the payment authority in order to transfer the information and make the purchase. Information about the purchase must also be saved in order to prove to the payment authority and to the customer that the purchase has been made correctly if questioned.

8.2 Communication methods

The communication from the mobile device to the MSP may use one of six technologies, these being speech, SMS, MMS, USSD, http and midlet. Each technology will be discussed briefly with benefits and disadvantages and how it could be implemented. When it comes to the risks, it mostly depends on whether the service uses GSM or GPRS but they might have some additional risks not covered in the general description. However, according to a few articles covering the security of these two technologies they are both vulnerable to eavesdropping, replay attacks, man-in-the-middle attacks, Denial of Service attacks and masquerade attacks[24][15][22][5].

Beginning with speech, in this case the communication is interpreted by an automatic phone service that communicates with the user, asking for the requested information and passing this forward as a message to the transaction server. Since the messages are only digits, there is no need for any speech recognition software; it is easier and faster to type the number on the keypad of the phone. On the way back, the data is interpreted and read aloud to the customer. This is very easy to understand and use, it requires a very low technical understanding and is useful to gain a larger group of customers. However, it is a very slow way to make the transaction in comparison with USSD or midlets but when the customers are used to the system; they might be open to change to a more effective way, as Midlets or SMS service.

In regards to security, the security of GSM can be questioned and the communication could be eavesdropped with equipment available to military, large companies and such likes in 2004[24]. With the current development, the same computation power will probably soon be available to the common user and might already be available for students at universities for example. Such institutions also often have the other equipment needed for monitoring radio communication and analyzing the result as well as the technical competence among senior students and staff. There is also a risk of physical eavesdropping, either by standing next to the person making the transaction or by using a high quality microphone directed at the front of the machine.

The next possible technology is SMS, a SMS server handles and interprets the SMS from the customer and passes the requested information on to the transaction server. On the way back, the data is sent as a SMS to the customer. This is easy and simple to do, however it has a few security aspects that makes it less useful. The biggest issue is the unreliability issue, SMS is a non-reliable service, it has no guaranties to be delivered or when it will be delivered.

Therefore it can produce a few problems, for example, dissatisfied customers who sent a message to buy an item but never received an answer, unsynchronized communication as the message to the transaction server came through but the reply to the customer never made it.

It also has a security issue in the mobile phone; every SMS is saved and if the service requires account information to be sent in the SMS, this information will be left on the mobile phone if the user does not actively delete it. MMS has the same features as SMS server but with the benefit of being able to send and receive sound and images, useful for implementing the dial tones and barcode transfer methods.

As for USSD, that variety uses the "Unstructured Supplementary Service Data" service that is available in any GSM phone. The service is operator specific and is handled by the MSP. In this case the user just types the code directly on the phone, just like dialing any phone number but starts the code with an asterisk. The code is then interpreted by the MSP and the information extracted is forwarded to the transaction server. This might be the simplest way, the request can be sent in just a few seconds if no security features are used and there is only static information sent. However, the common return path of these messages is by SMS which returns the reliability issues.

USSD also has another drawback, as the codes used are operator specific, there has to be an agreement between all MSP in order to create a common platform, independent of the users' choice of MSP. This might work in a country perspective, although finding a common agreement between operators on a larger level, say a group of countries, might prove impossible. It also involves more work for the MSP, resulting in higher cost for a third party supplying the service. This option might be best used by a MSP, using this service as a benefit to their users and to attract customers of other MSP to get them to switch operator.

Another alternative is using http for the transactions, the customer uses a browser on the mobile device and sends the information needed with the GPRS service to the web interface of the transaction server. The response is an automatically generated web page with the message to the machine. This involves a web server on the transaction server which might open up to common web server attacks if not configured correctly.

The last option is using midlets to send and receive information. The user installs a program on the mobile device and uses this to send information to the transaction service with the use of the GPRS service from the MSP. This has a few advantages to the http variety as a midlet can easily save information such as history of purchases, list of favorite machines and so on. It is however important to consider the risk of reverse engineering so that no security is built in to the application itself. The transaction server might also be vulnerable to common server attacks such as port scanning, buffer overflows and Denial of service.

8.3 Transfer methods

In order to transfer the message between the machine and the mobile device, there are a few methods that could be used that include more or less work for the customer. The lists of methods are the ones that are common on mobile phones which are expected to be the primary mobile device used. The methods are keypad, infrared, Bluetooth, visual and dial tones. All methods present their own advantages and disadvantage and are covered separately, beginning with the keypad.

With keypads, the message is transferred by hand, entered on the keypad of mobile device or the machine. As this is typed by the customer, it puts a large constraint on the number of digits and the characteristics of the code, typing alphanumeric characters takes longer time than typing numeric characters for example. How many characters a customer is willing to enter is hard to predict and needs to be evaluated, but it is safe to say that the fewer the better so the code needs to be as short as possible. The biggest advantage of this method is that it is very easy, just punch in the numbers when asked for them and every mobile phone has a way to enter a numerical code. The downside is of course the mentioned restraints on the length

of the number and the time aspect; it takes longer to enter them manually than to send them by IR or Bluetooth.

The method presents a few risks, the primary being a replay attack by copying the code when the customer enters it, either by standing in a good view or by using a camera to record all transactions. By using a technique commonly used to attack cash dispensers the code could also be copied but done right it could instead be used in a man-in-the-middle attack. This is done by attaching a new keypad on top of the real keypad. It is also possible to do a DOS attack by making the keypad useless, for example by smashing or pouring glue over it. This method is probably the most susceptible to sporadically brute force attacks as it does not demand anything but time and no technological know-how.

The next studied method is infrared; the message is transferred between the IrDA port on the mobile device and the responding port on the machine. This technology is quite common on mobile devices, in 2003 almost 50% of the mobile phones sold were equipped with IrDA but it might soon be replaced by wireless options that work without line-of-sight. The line-of-sight issue is a problem with the technology; it can not be used unless the communicating parties are very close and with no objects in the way. But it does not have any real constraints on the length or type of the message; it is fast enough to send whatever needed within a few seconds, within reasonable limits. In comparison to Bluetooth, this method has the downside of using neither encryption nor authentication in the protocol.

It is possible to eavesdrop on the communication by detecting reflected light and thereby do a replay attack. It would also be feasible to attach a new IrDA port on top of the real port to record the communication and use later as a man-in-the-middle attack. Brute force attack could also be possible depending on implementation and a spray can of paint can be used to do a DOS attack in a second.

Then there is Bluetooth, the message is transferred by the Bluetooth function on the mobile device and on the machine. This method could be the simplest for the user if it could be made to work automatically and it also provides a secure transfer between the mobile device and the machine. A potential problem might be to find the right connection to the machine and to verify that it is not an attacker spoofing the machine identification in order to gain user data. This potential problem leads to a risk of man-in-the-middle attacks. The Bluetooth protocol also has risks that make it possible to eavesdrop on the communications and to do a DOS attack. A brute force attack is also theoretically possible but might be practically unfeasible due to the possible length of code.

The visual method refers to using barcodes; the message is transferred by holding up the mobile device's display against the machine's barcode scanner while displaying the message in form of a picture. This can easily be used with MMS as communication method or by WAP or Midlet. If the machine is equipped with a display capable of showing barcodes, the barcode could be read with an ordinary mobile phone equipped with a camera [13]. This technology does not put a big restriction on the number of characters to send and the transfer can be done quickly.

In case of barcodes being used in both directions, the user needs to stand by the machine during the whole transfer and the communication should therefore be instant, ruling out the MMS as a communications mean. A WAP page or a Midlet application might work very well for this purpose however. The method might be vulnerable to replay and man-in-the-middle attacks by putting a miniature camera on the machine beside of or in front of the real camera. A brute force attack is possible by putting, for example, a laptop screen in front of the machine and let it display different barcodes until a valid code is found.

The last method covered is the oldest, by using dial tones; the message is transferred by holding the microphone to the speaker of the other device and vice versa. This is the same method used in early modem technologies when you put the phone on special unit in order to convert the sounds to electronic data. This is a possible way to transfer the data but it is not very convenient or safe, in a loud area it might be too much interference and it might be hard to get the right distance between microphone and speaker. In an area with low noise it might instead be possible to eavesdrop using a microphone. The possible attacker might also use brute force to try to gain a valid code.

The Infrared and Bluetooth methods has two advantages against the others, they have no real restriction on the information to be transferred. This means that the information can be any characters available to the device and in lengths far longer than the other methods which make brute force attacks unfeasible.

8.4 Transfer data

The data to send can be very different between implementations, with different views on security and risk management. Some part of the data should be encrypted to enhance security. Some of the data that might be relevant to send between the machine and the transaction server is covered in this section. The primary information needed to make a transaction is the buyer, the seller, the amount and how the money should be transferred. The how is covered in the payment section and is not relevant to send each time.

The amount however is critical in order to make a correct payment. If the machine has items with different costs or if the system allows purchases of many items at the same time, this is needed to include. Should the machine only have the same valued items and not allow for more than one item per sale, this field may be excluded. When sending the cost in the message there is a risk, depending on the rest of the implementation, that the value could be modified in order to pay less for an item and if the transactions are monitored, it could be used to gather information about how much money each customer is spending on vending machines. The seller will in this case be the machine; therefore a machine identification number might be needed to identify the seller correctly. The system can also be designed to ignore the specific machine that sold the item and just transfer the money to the company.

The machine identification serves also another purpose however, together with encryption it might be used to identify which key is to be used for the rest of the communication. If the response to the machine in some way depend on the machine identification number, it might be possible to change this number to gain items from another machine.

The most critical information is the user identification, an account identification number for example together with a personal identification number to verify the identity of the customer. If this information can be known and changed, it could be used to charge items to another customer so this has to be implemented in a safe way. If the communication could be read, even if it can not be modified, it would still be a threat, in this case against privacy as customers can be pinpointed to certain machines at certain times.

In order to verify that the transaction has been approved, the machine needs some sort of response, a payment status. This is possibly the most important information in the eyes of the attacker as this could be used to verify a transaction that actually failed if the value could be modified to a valid value. The monitoring of this value might also be a threat to privacy as this gives information to the viewer when and if a customer gets a payment denied, which might imply that the customer has problems to pay their bills.

Other information that could be useful to send is a checksum to verify the entered code, the number of remaining items, which items that were sold in this purchase and perhaps a timestamp to stop replay attacks. The number of remaining items is very useful in order to optimize the supply chain but might also give competing business information needed to compete in this specific market if it can be read. If it could be changed, it could be used to sabotage the supply chain of the attacked company. The same risk goes for sending the identification of the items that were sold in each purchase and if the price is based on the sold item, a possible change in this value results in another price.

When using for example keypad as a transfer method it would be practically impossible to transfer all this data and it has to be compressed as much as possible and all information that is not needed should be discarded in order to make the method usable.

8.5 Security aspects

The security aspects mainly consist of the possibility of encrypting the communication between the machine and the transaction server in order to keep the information safe. Tamper resistance and timestamps will also be covered briefly[1]. When it comes to cryptography, it depends on the properties of the used embedded system, different sorts of cryptographic algorithms can be used in order to keep the confidentiality of the messages. There are many available algorithms and any one that is considered safe and runs quickly on the embedded system could be a good choice.

As the size of the transferred data is very small and with only digits in some transfer methods, there is a serious risk that the key will be discovered should the key remain constant and have the same length of the encrypted information. As the communication is very limited between the machine and the transaction server, there is no reasonable way to implement a negotiated one time session key in the current session. One could however use the current transfer to negotiate the key for the next session. This however presents another problem as the transfer must come in a strict order to be readable which can not be guaranteed.

Another solution is to use a one-time pad to encrypt the message with. This method would have the smallest requirement on the embedded system's CPU power but require a certain amount of memory to store the pad in, depending on the amount of data to be sent in each transfer. In the threat analysis, the system has been analyzed as having encrypted information but also covers the risks when not having encrypted the information. There is also a risk with encryption giving a false sense of security, there might be a possibility to decrypt it or the keys might have been compromised. It is also important to remember that just because the keys are safe today does not guarantee that they are safe tomorrow; if the secret information has been recorded it might be readable at a later time.

Regarding keys, it might also be usable to use asymmetric keys in order to make it harder to crack the encryption as the number of messages with a common key possible to analyze are divided in half. Given the amount of memory is sufficient, the fastest and most secure key would be the one time pad. This must however then be large enough to encrypt all purchases until it can be replaced. This might be a waste of resources for this small valued transactions and it would be more effective to make it reusable. Making the key constant is might open up to cryptanalysers as the messages will be very similar and short if the message shall be able to be transferred by keypad. Should that restriction be invalid, and then there could be a key long enough to make it secure and still keep it within sending limits. However, the message might not have enough relevant information to encrypt and be forced to encrypt random numbers to keep the length. It is also important to remember that it is easy for the attacker to gather information to analyze, just order a few items, either of the same kind to

view similarities or different items in order to view differences. It is also possible for the attacker to send a chosen text to the transaction server to study the result.

Should a constant key be used, there needs to be some way to stop a possible replay attack, both the code from the machine to transaction server and the code back again needs to only be valid once. This could be done either by adding a random number sequence or by adding the time before encryption. The downside is that this makes the message longer and it might lead to an easier cryptanalysis in combination with a brute force attack if only certain characters are affected by the timestamp.

In order to keep the keys secret, there is also a need for tamper resistance, the physical construction of the embedded machine and the transaction server should be done so that no information can be extracted from the system without authorization or an effort that exceeds the value of the information gained. As the keys are machine specific, the value of the keys is the contents of the machines available for sale. Another issue is the resistance against tampering with the purchase order, the system can not depend on that the previous purchase being valid and if the sequence order is totally disordered, it should reset itself while still being non predictable.

8.6 Maintenance

In the need of manually updating keys, the keys should be generated at the transaction server and installed on this first but wait for a signal before switching to the new keys. The keys to all machines that shall be updated on this route should then be copied to a memory stick. The update on the vending machine should preferably be accomplished at the same time as the machine gets refilled with items. This might then be done by unlocking the service panel and inserting the USB memory stick and press an update button.

After inserting a code, the embedded system copies the information to memory and starts using the new keys. When this is done, the display should print status of the update to let the service personal update the transaction server. As the machine is finished with updating, the service personal sends a message to the transaction server to activate the new keys and the system is then back online. It should be impossible to copy the current key from the machine; it should only be possible to insert a new one. If a key chosen by the attacker could be entered, this will probably not correspond to the key available at the transaction server and the system will stop working.

If the system is dependant on the sequence in which the messages occur, a malicious user managing to acquire an item through a brute force attack will make the system unsynchronized and there needs to be a way for the system to resynchronize. As there is no free communication between the machine and the transaction server, the synchronization must either be on a specific interval or as a request in a message. This however proposes a risk, if it synchronizes to the same value each time or the value can be predicted in any other way, a forced synchronization will be useful to make a replay attack.

9 SYSTEM CHOICE

The construction of the design for the analyzed system was done by specifications from Johan Persbeck at Cybercomgroup Sweden South in Karlskrona and will not be included in this thesis for copyright reasons. The system was designed with previous systems and the conducted threat analysis in mind, using selected technologies from those described in chapter 8 after weighing their advantages and disadvantages against each other. For the purpose of understanding the chapter on attack trees, some knowledge about the system is however required.

9.1 Analysed system

Although the system proposed by Azami and Tanibian in 2004 is not exactly the same, it builds on the same principles and can be used in order to get a basic understanding of how the system works. The following section is a short summary of the system described in that paper using the manual mode as this would be the most critical way of transferring the data and was therefore used in the threat analysis. There are a few differences between this and the constructed system as the system was constructed from scratch but the attack tree is valid for their system also with the addition of an authentication that is done in the mobile device upon payment. The authentication requires a code that is known only by the customers themselves, and those trusted by each customer, and the transaction server. A figure of the communication flow in their system is presented below.

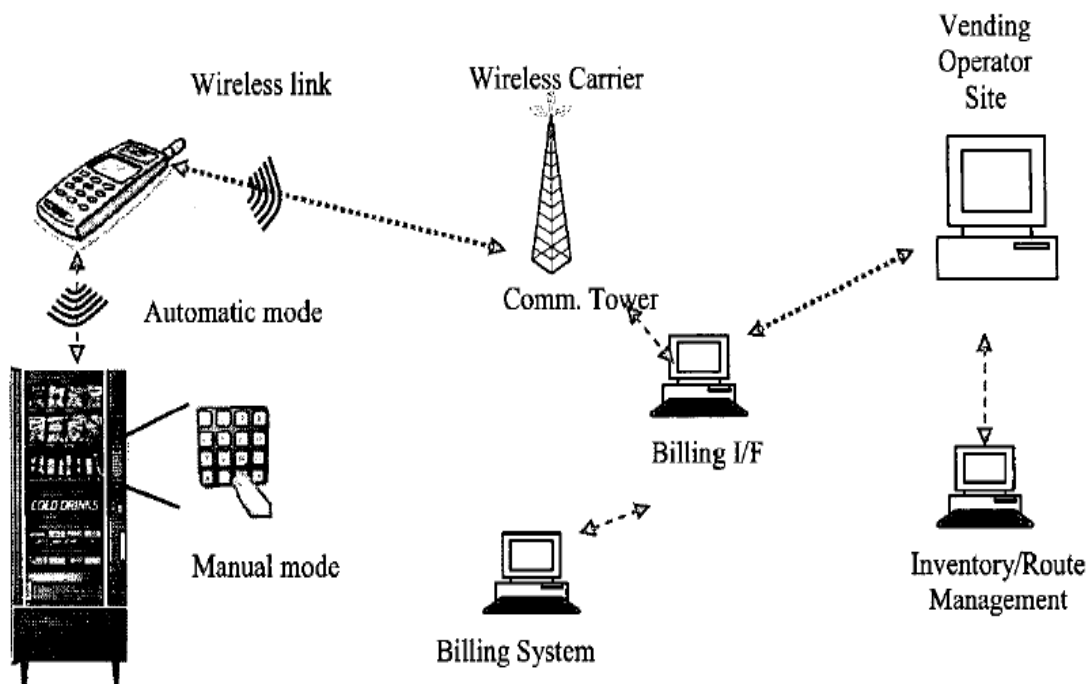


Figure 1: Communication flow in the analyzed system

The system described by Azami and Tanibian was designed for the use on vending machines that have no permanent data connection to the company and where the normal payments are for the cost of a soda. The transaction server, here called the Back-End Server Side (or Billing I/F in the picture), does not store any credit card data that can be used for other purchases but uses billing as payment method. The vending machine generates two messages, the Query Packet and the Reply Packet, and the Query Packet is transferred to the mobile device and the machine then awaits the Reply Packet. The packets are compressed,

encrypted and a cyclic redundancy check code is attached to the message for error detection before being sent from either party. When the Billing System receives the Query Packet, it authorizes the transaction if possible and sends the Reply Packet back to the mobile device. The customer transfers the Reply Packet to the machine and which either approves or denies the request. The data included in the Query Packet here includes transaction based data such as machine number, product code and price. The user identification is done by checking caller Id of the user phone. The Query Packet also includes information useful for the supply chain in order to optimize supply routes.

This system can hence forward be considered as the constructed system.

9.2 Reference system

The reference system is based on the design of the proposed system. The difference lies in the origin of communication and the customer handling in the machine. The communication device that was supplied by the customer in the constructed system is in this case integrated into the machine with the customer having no access to it. Instead of the account identification being associated with the mobile device, the customer now has a token that holds the account identification. This represent about the same difficulty to come by as acquiring the mobile device of a customer. The customers still have their own authorization code that is to remain secret from any other users not trusted by the customer. So the authentication from the customers still consist of a personal token only owned by the customer together with information only known by the customer. The difference here is that instead of the customer sending the information with their mobile device; it is now sent by the machine. The customer creates an order, provides the token and enters the PIN. The information is then sent from the machine to the MSP and forwarded to the transaction server. The information is handled the same way and the response is sent to the machine. Using a separate connection for communication in a vending machine might cost more to implement and run than the expected gain but it serves to prove the differences in threats between customer based communication and seller based communication. It is assumed that the machine is accessible at any time from the Internet via the data connection.

10 COMPARATIVE THREAT ANALYSIS

10.1 Introduction

This threat analysis has been based on the method described by Bruce Schneier as Attack tree [17][18]. It is a methodical way to display the threats to a system and makes it easy to see where it would be most effective to insert defensive measures to each threat. The method can be used to quantify the cost of different attacks and relate these costs to the cost of the defensive measures. In short, the method focuses on the goals of an attack uses these as base for finding ways to attack the system. Each attack is broken down to more requirements to accomplish the attack until a reasonable level has been reached.

10.1.1 Scales

In order to get a more quantified comparison instead of just subjective reasoning, the effects to the company if the goals should be accomplished have been quantified. The scale used to quantify is in three steps:

Negligible – Effect will hardly be noticed

Small – The effect is noticeable but not serious and does not affect the future of the company

Large – The effect is serious and might affect the future of the company

It is important to note that this scale depends highly on the size of the company; in a small company a small loss will create a larger effect than in a large company.

Each node in the attack trees will also have a value associated with it that represents the difficulty of accomplishing the attack node. The scale for this is as follows:

1. Easy – Can be done by anyone/Likely
2. Medium – Requires some resources or technical know-how/not likely
3. Hard – Can only be done with large resources and/or a deep technological understanding/highly unlikely

When all nodes must be fulfilled in order to fulfill the parent node (AND), the parent node will have the value of the highest of its children. If only one node must be fulfilled in order to fulfill the parent, the parent node will have the value of the smallest of its children.

Environmental and undeliberate threats have also been included in this analysis even though they can not be strictly considered as an attack that is per definition deliberate.

Each goal will be analyzed first for the constructed system and then for a reference system with a short discussion after each goal.

10.1.2 Goals

The attack goals can be categorized in to two categories, theft and sabotage. The difference between these two is mainly that the theft is probably done for financial gain of the attacker while sabotage has a larger focus on financial loss for the company. The analyzed goals are:

1. Acquire one or more items from one or more machines without paying.[Negligible]
2. Acquire personal or company information such as purchase information and payment information about a small number of customers.[Negligible]
3. Acquire personal or company information such as purchase information and payment information about a large number of customers.[Large]
4. Sabotage the service for a machine and render purchases from this machine impossible.[Small]
5. Sabotage the service for the transaction server.[Large]
6. Sabotage the service for a customer.[Negligible]
7. Sabotage the supply service.[Negligible]

These effects are based on a fictional company with 100 machines.

10.2 Compared systems

The designs of the constructed systems are not covered in this thesis as mentioned in the chapter on system choice. As stated there, the system proposed by Azami and Tanabian in 2004 can be used to understand the threat analysis, adding the use of authentication and using their manual mode. See chapter 9 for more information on this system and the reference system or read their paper[3].

10.3 Attack trees

10.3.1 Acquire item(s)

Acquire one or more items from one or more machines without paying. This result in a small loss for the company running the system if accomplished only once every now and then but will make the system less profitable if it is possible to abuse the system at a regular basis or using an automated method.

Constructed system {Easy}:

1. Use someone elses account to pay(OR){Easy}
 1. Buy the item from the mobile device used by the target(AND){Easy}
 1. Acquire access to the mobile device(OR){Easy}
 1. Steal while the target is logged in {Medium}
 2. Ask to lend {Easy}
 3. Buy {Medium}
 4. Hack the mobile device using remote access {Hard}
 2. Acquire the PIN(OR){Easy}
 1. Monitor the target as the code is entered(OR){Easy}
 1. Stand in a viewing angle and range to the target {Easy}
 2. Place a camera so that the code can be seen when entered {Medium}
 2. Eavsdrop on the communication(OR){Hard}
 1. Listen on the communication between the customer and the MSP {Hard}
 2. Monitor any of the devices relaying the information at the MSP {Hard}
 3. Listen on the communication between the MSP and the transaction server {Hard}
 3. Acquire the code from the database on the transaction server(OR){Hard}
 1. Hack the transaction server {Hard}
 2. Bribe/threaten/decieve someone with access to the database {Hard}
 3. Be an authorized employee {Hard}
 2. Buy the item from another device using the personal information from the target(OR){Easy}
 1. Acquire the information from the target(AND){Easy}
 1. Acquire the account identification(OR){Easy}
 1. Acquire the mobile device and copy the information(OR){Easy}
 1. Steal {Medium}
 2. Ask to lend {Easy}
 3. Buy {Medium}

2. Convince the target to surrender the information(OR){Medium}
 1. Threaten {Medium}
 2. Bribe {Medium}
 3. Decieve {Medium}
3. Hack the mobile device using remote access {Hard}
2. Acquire the PIN(OR){Easy}
 1. Monitor the target as the code is entered(OR){Easy}
 1. Stand in a viewing angle and range to the target {Easy}
 2. Place a camera so that the code can be seen when entered {Medium}
 2. Convince the target to surrender the information(OR){Medium}
 1. Threaten {Hard}
 2. Bribe {Hard}
 3. Decieve {Medium}
2. Acquire the information from the communication during a purchase(OR){Hard}
 1. Listen on the communication between the customer and the MSP {Hard}
 2. Monitor any of the devices relaying the information at the MSP {Hard}
 3. Listen on the communication between the MSP and the transaction server {Hard}
3. Acquire the information from the database on the transaction server(OR){Hard}
 1. Hack the transaction server {Hard}
 2. Bribe/threaten/decieve someone with access to the database {Hard}
 3. Be an authorized employee {Hard}
3. Construct a fake method of input for the code that replaces the legitimate method. {Medium}
4. Fool the customers to use a false transaction server to steal the codes(AND){Medium}
 1. Get the customers to use a false transaction server(OR){Medium}
 1. Change the routing tables at the MSP {Hard}
 2. Make the customers change their adress to the transaction server manually {Medium}
 3. Make the customers run a program that changes the adress automatically {Medium}
 2. Program the false server to copy and forward all information to real transaction server {Easy}
 3. Do not send the reply to the customer for those codes that should be used by attacker {Easy}
5. Steal wanted codes when sent back to the customers(AND){Hard}
 1. Insert a false router between the transaction server and the MSP {Hard}
 2. Route unwanted codes as usual but do not send wanted codes to the correct adress {Medium}
 3. Have a server recieve wanted codes and send responses {Easy}
2. Insert a valid code that does not come from the transaction machine(OR){Hard}
 1. Create a valid code(AND){Hard}
 1. Acquire the key(OR){Hard}
 1. Hack the transaction server {Hard}

2. Bribe/threaten/decieve someone with access to the key database {Hard}
3. Be an authorized employee {Hard}
4. Extract the key from the embedded system in the machine {Hard}
5. Monitor the entered codes together with the order and analyse it until a pattern can be found {Hard}
2. Acquire the encryption method (OR) {Medium}
 1. Hack the transaction server or a machine that holds the code to the encryption {Hard}
 2. Bribe/threaten/decieve someone with access to the information {Medium}
 3. Be an authorized employee {Hard}
 4. Extract the information from the embedded system {Hard}
 5. Blackbox test using the key, the code and the result {Medium}
3. Acquire the code that should be encrypted(OR){Medium}
 1. Hack the transaction server {Hard}
 2. Bribe/threaten/decieve someone with access to the information {Medium}
 3. Be an authorized employee {Hard}
 4. Extract the information from the embedded system {Hard}
 5. Use the key, the result and the reversed encryption algorithm {Hard}
2. Bruteforce attack a valid code {Hard}
3. Use a software error(OR){}
 1. Use a deliberate error(backdoor)(OR){}
 1. Bribe/threaten/decieve one of the legitimate programmers to insert a backdoor {Hard}
 2. Get access to implement a backdoor {Hard}
 3. Do blackbox testing to find a backdoor {Hard}
 4. Get access to the code to find a backdoor(OR) {Hard}
 1. Bribe/threaten/decieve one of the programmers {Hard}
 2. Hack a computer with the code on it {Hard}
 3. Be an authorized employee {Hard}
 4. Get the code from the embedded system in the machines(AND) {Hard}
 1. Get access to the embedded system {Hard}
 2. Extract the code from the embedded system {Hard}
 2. Use one that has been created by accident i.e a bug(OR) {Medium}
 1. Do blackbox testing to find an error {Hard}
 2. Get access to the code to find an error(OR) {Medium}
 1. Bribe/threaten/decieve one of the programmers {Medium}
 2. Hack a computer with the code on it {Hard}
 3. Be an authorized employee {Hard}
 4. Get the code from the embedded system in the machines(AND) {Hard}
 1. Get access to the embedded system {Hard}
 2. Extract the code from the embedded system {Hard}
4. Call customer service to get a refund(OR){Easy}
 1. Claim the code was never delivered(AND) {Medium}
 1. Prevent the mobile device to send an aknowledgement that the code has been recieved {Medium}
 2. Claim the item was not delivered when the code was entered on the machine {Easy}
5. Register an account with false name(AND){Medium}

1. Get access to all the needed information about the false name{Medium}
2. Use a mobile device that can not be traced to the attacker for purchases{Easy}
6. Change the billing information for the specific account(OR){Medium}
 1. Bribe/threaten/deceive one of the staff with access to the billing database{Medium}
 2. Hack a computer with access to the billing database{Hard}
 3. Be an authorized employee{Hard}

Reference system{Easy}:

1. Use someone else's account to pay(OR){Easy}
 1. Buy the item using the personal information from the target(OR){Medium}
 1. Acquire the information from the target(AND){Medium}
 1. Acquire the account identification(OR){Medium}
 1. Acquire the mobile device and copy the information(OR){Hard}
 1. Steal{Hard}
 2. Ask to lend{Hard}
 2. Convince the target to surrender the information(OR){Medium}
 1. Threaten{Medium}
 2. Bribe{Medium}
 3. Decieve{Medium}
 2. Acquire the PIN(OR){Easy}
 1. Monitor the target as the code is entered(OR){Easy}
 1. Stand in a viewing angle and range to the target{Easy}
 2. Place a camera so that the code can be seen when entered{Easy}
 2. Convince the target to surrender the information(OR){Medium}
 1. Threaten {Medium}
 2. Bribe{Medium}
 3. Decieve{Medium}
 2. Acquire the information from the communication during a purchase(OR){Hard}
 1. Listen on the communication between the machine and the MSP{Hard}
 2. Monitor any of the devices relaying the information at the MSP{Hard}
 3. Listen on the communication between the MSP and the transaction server{Hard}
 3. Acquire the information from the database on the transaction server(OR){Hard}
 1. Hack the transaction server{Hard}
 2. Bribe/threaten/deceive someone with access to the database{Hard}
 3. Be an authorized employee{Hard}
 2. Steal accounts by using recording equipment on the machine(AND){Hard}
 1. Construct a fake method of input for the code that replaces the legitimate method.{Medium}
 2. Place a false token reader on the machine to copy the token{Hard}
 3. Make the machine use a false transaction server to steal the codes(AND){Hard}
 1. Get the machine to use a false transaction server(OR){Hard}
 1. Change the routing tables at the MSP{Hard}
 2. Change the address on the embedded system{Hard}
 2. Program the false server to copy and forward all information to real transaction server{Easy}
 3. Do not send the reply to the machine for those codes that should be used by attacker{Easy}
 4. Steal wanted codes when sent back to the customers(AND){Hard}
 1. Insert a false router between the transaction server and the MSP{Hard}

2. Route unwanted codes as usual but do not send wanted codes to the correct address {Medium}
3. Have a server receive wanted codes and send responses {Easy}
2. Insert a valid code that does not come from the transaction machine (OR) {Medium}
 1. Create a valid code (AND) {Hard}
 1. Acquire the key (OR) {Hard}
 1. Hack the transaction server {Hard}
 2. Bribe/threaten/deceive someone with access to the key database {Hard}
 3. Be an authorized employee {Hard}
 4. Extract the key from the embedded system in the machine {Hard}
 2. Acquire the encryption method (OR) {Medium}
 1. Hack the transaction server or a machine that holds the code to the encryption {Hard}
 2. Bribe/threaten/deceive someone with access to the information {Medium}
 3. Be an authorized employee {Hard}
 4. Extract the information from the embedded system {Hard}
 5. Black box test using the key, the code and the result {Medium}
 3. Acquire the code that should be encrypted (OR) {Medium}
 1. Hack the transaction server {Hard}
 2. Bribe/threaten/deceive someone with access to the information {Medium}
 3. Be an authorized employee {Hard}
 4. Extract the information from the embedded system {Hard}
 5. Use the key, the result and the reversed encryption algorithm {Hard}
 2. Brute force attack a valid code {Medium}
3. Use a software error (OR) {Easy}
 1. Use a deliberate error (backdoor) (OR) {Hard}
 1. Bribe/threaten/deceive one of the legitimate programmers to insert a backdoor {Hard}
 2. Get access to implement a backdoor {Hard}
 3. Do black box testing to find a backdoor {Hard}
 4. Get access to the code to find a backdoor (OR) {Hard}
 1. Bribe/threaten/deceive one of the programmers {Hard}
 2. Hack a computer with the code on it {Hard}
 3. Be an authorized employee {Hard}
 4. Get the code from the embedded system in the machines (AND) {Hard}
 1. Get access to the embedded system {Hard}
 2. Extract the code from the embedded system {Hard}
 2. Use one that has been created by accident i.e. a bug (OR) {Easy}
 1. Do black box testing to find an error {Easy}
 2. Get access to the code to find an error (OR) {Medium}
 1. Bribe/threaten/deceive one of the programmers {Medium}
 2. Hack a computer with the code on it {Hard}
 3. Be an authorized employee {Hard}
 4. Get the code from the embedded system in the machines (AND) {Hard}
 1. Get access to the embedded system {Hard}
 2. Extract the code from the embedded system {Hard}
4. Call customer service to get a refund (OR) {Easy}
 1. Claim the item was not delivered when the code was entered on the machine {Easy}
5. Register an account with false name (AND) {Medium}
 1. Get access to all the needed information about the false name {Medium}
6. Change the billing information for the specific account (OR) {Medium}

1. Bribe/threaten/deceive one of the staff with access to the billing database {Medium}
2. Hack a computer with access to the billing database {Hard}
3. Be an authorized employee {Hard}

10.3.1.1 Comparison

There are quite a few differences in the attack trees here and the differences indicates that the constructed system is easier to steal from other customers while it is on the reference system easier to steal directly from the system by using a brute force attack against the always connected machine.

10.3.2 Small scale privacy attack

Acquire personal or company information such as purchase information and payment information about a small number of customers. This might not be that serious and can easily be handled as long as the company supplying the service can deny responsibility but can lead to a loss of customer in the case that the company is responsible for making the information available.

Constructed system {Medium}

1. Get the information from the transaction server(OR) {Hard}
 1. Bribe/threaten/deceive one in the authorized staff to surrender the information {Hard}
 2. Be an employee with access to the data {Hard}
 3. Hack the transaction server or any other machine with access to the information {Hard}
2. Get the information about purchases from the communications(OR) {Hard}
 1. Listen on the communication between the machine and the MSP {Hard}
 2. Monitor any of the devices relaying the information at the MSP {Hard}
 3. Listen on the communication between the MSP and the transaction server {Hard}
3. Convince the customers to give the information(OR) {Medium}
 1. Make the customer answer a false survey {Medium}
 2. Use a phishing attack to make the customers release information {Medium}
4. Unintentional disclosure {Hard}

Reference system {Medium}:

1. Get the information from the transaction server(OR) {Hard}
 1. Bribe/threaten/deceive one in the authorized staff to surrender the information {Hard}
 2. Be an employee with access to the data {Hard}
 3. Hack the transaction server or any other machine with access to the information {Hard}
2. Get the information about purchases from the communications(OR) {Hard}
 1. Listen on the communication between the machine and the MSP {Hard}
 2. Monitor any of the devices relaying the information at the MSP {Hard}
 3. Listen on the communication between the MSP and the transaction server {Hard}
3. Convince the customers to give the information(OR) {Medium}
 1. Make the customer answer a false survey {Medium}
 2. Use a phishing attack to make the customers release information {Medium}
4. Unintentional disclosure {Hard}

10.3.2.1 Comparision

The easiest way to get the information is to decieve the customer with the wanted information by, for example, present the customer with a fake offering of free items if the wanted information is provided to something that looks like the company. However, there is a small difference here between the two systems, the constructed system can be attacked by the mobile device directly. The other way, that works on the reference system also, is using an external phising attack by, for example, posting a link on the vending machine. The differences does not however make any difference in the result of the comparision as a whole.

10.3.3 Large scale privacy attack

Acquire personal or company information such as purchase information and payment information about a large number of customers. Can be considered very serious for a company and might lead to a large loss of customers and business trust, resulting in a large loss of income.

Constructed system {Hard}:

1. Get the information from the transaction server(OR) {Hard}
 1. Bribe/threaten/decieve one in the authorized staff to surrender the information {Hard}
 2. Be an employee with access to the data {Hard}
 3. Hack the transaction server or any other machine with access to the information {Hard}
2. Get the information about purchases from the communications(OR) {Hard}
 1. Listen on the communication between the customer and the MSP {Hard}
 2. Monitor any of the devices relaying the information at the MSP {Hard}
 3. Listen on the communication between the MSP and the transaction server {Hard}
3. Unintentional disclosure {Hard}

Reference system {Hard}:

1. Get the information from the transaction server(OR) {Hard}
 1. Bribe/threaten/decieve one in the authorized staff to surrender the information {Hard}
 2. Be an employee with access to the data {Hard}
 3. Hack the transaction server or any other machine with access to the information {Hard}
2. Get the information about purchases from the communications(OR) {Hard}
 1. Listen on the communication between the machine and the MSP {Hard}
 2. Monitor any of the devices relaying the information at the MSP {Hard}
 3. Listen on the communication between the MSP and the transaction server {Hard}
3. Unintentional disclosure {Hard}

10.3.3.1 Comparision

This attack goal is not really dependant on any of the differences in the systems and all the nodes found to attack the goal are hard to accomplish. The only major difference from the previous goal is the effect of the attack, a lot of users' information lost can be catastrophic if caused by a company.

10.3.4 Sabotage of a machine

Sabotage the service for a machine and render purchases from this machine impossible. This is a goal that might not be considered as doing any real harm from an attacker and might be done by someone who feels cheated by the machine or the system as a revenge action. This can be considered as something that might occur at regular intervalls.

Constructed system {Easy}:

1. Make the machine useless(OR){Easy}
 1. Try to freeze the machine by inserting an unhandled input as 1000 characters for example{Hard}
 2. Disable the means for inserting code{Easy}
 3. Disable the display {Easy}
 4. Unplug the power{Easy}
 5. Create a powersurge or power fluctuations that destroys the embedded system{Hard}
 6. Destroy the embedded system physically{Hard}
 7. Change the cryptography keys the machine{Hard}
 8. Steal vital parts of the machine or all contents{Medium}
 9. Alter or remove the machine number on the attacked machine{Easy}
2. Stop correct responses from the transaction server to this machine(OR){Hard}
 1. Delete or change the machine number in the database {Hard}
 1. Bribe/threaten/decieve one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee{Hard}
 2. Modify the software to ignore requests from the specific machine(OR){Hard}
 1. Bribe/threaten/decieve one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee{Hard}
 3. Change the cryptography keys on the transaction server(OR){Hard}
 1. Bribe/threaten/decieve one of the authorized staff{Hard}
 2. Hack the transaction server{Hard}
 3. Be an authorized employee{Hard}
 4. Make the keys unsynchronized by changing the subkey index(OR){Hard}
 1. Bribe/threaten/decieve one of the authorized staff{Hard}
 2. Hack the transaction server{Hard}
 3. Be an authorized employee{Hard}
 5. Disturb the communication between the MSP and the mobile device by a local Denial of Service attack against the MSP{Hard}
3. Make the machine useless in the mobile devices(AND){Hard}
 1. Create a false client software that stops or alters communications from certain machines{Hard}
 2. Convince a majority of the customers to install the false software{Hard}
4. System acts unpredictable(OR){Hard}
 1. Bad design of system{Hard}
 2. Bad programming of system{Hard}
 3. User error{Hard}
5. Enviromental disturbance(OR){Hard}
 1. Electrical disturbance{Hard}
 2. Electrical interruption{Hard}
 3. Hardware failure{Hard}
 4. Telecommunications interruption{Hard}

Reference system {Easy}:

1. Make the machine useless(OR){Easy}
 1. Try to freeze the machine by inserting an unhandled input as 1000 characters for example{Easy}
 2. Do a Denial of Service attack against it from the Internet{Easy}
 3. Disable the means for input of code{Easy}
 4. Disable the display {Easy}
 5. Unplug the power{Easy}

6. Create a power surge or power fluctuations that destroys the embedded system {Hard}
7. Destroy the embedded system physically {Hard}
8. Change the cryptography keys the machine {Hard}
9. Steal vital parts of the machine or all contents {Medium}
2. Stop correct responses from the transaction server to this machine(OR) {Hard}
 1. Delete or change the machine number in the database {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
 2. Modify the software to ignore requests from the specific machine(OR) {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
 3. Change the cryptography keys on the transaction server(OR) {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
 4. Make the keys unsynchronized by changing the sub key index(OR) {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
 5. Disturb the communication between the MSP and the machine by a local Denial of Service attack against the MSP {Hard}
3. System acts unpredictable(OR) {Hard}
 1. Bad design of system {Hard}
 2. Bad programming of system {Hard}
 3. User error {Hard}
4. Environmental disturbance(OR) {Hard}
 1. Electric disturbance {Hard}
 2. Electric interruption {Hard}
 3. Hardware failure {Hard}
 4. Telecommunications interruption {Hard}

10.3.4.1 Comparison

The easiest way is the same for both systems, destroy the input/output systems on the machine. However, the reference system here has one large negative issue, it can be attacked from distance using a Denial of Service attack against the connection connecting the machine to the transaction server, making the system more vulnerable to large scale attacks from a distance.

10.3.5 Sabotage of transaction server

Sabotage the service for the transaction server. This goal has serious consequences as it will deny all customers service for as long as the attack is successful resulting in a large loss of income.

Constructed system {Medium}:

1. Modify or destroy the software on the transaction server(OR) {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
2. Modify or destroy the data(OR) {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}

3. Be an authorized employee {Hard}
3. Modify or destroy the communication (OR) {Medium}
 1. Change existing routing tables to stop traffic from reaching the transaction server {Hard}
 2. Insert a false router on the communication line {Hard}
 3. Change address in the client software to a false address {Hard}
 4. Physically destroy the communication line from the transaction server {Hard}
 5. Do a Distributed Denial-of-Service attack against the transaction server {Medium}
4. System acts unpredictable (OR) {Hard}
 1. Bad design of system {Hard}
 2. Bad programming of system {Hard}
 3. Staff user error {Hard}
5. Environmental disturbance (OR) {Hard}
 1. Electrical disturbance {Hard}
 2. Electrical interruption {Hard}
 3. Hardware failure {Hard}
 4. Telecommunications interruption {Hard}

Reference system {Medium}:

1. Modify or destroy the software on the transaction server (OR) {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
2. Modify or destroy the data (OR) {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
3. Modify or destroy the communication (OR) {Medium}
 1. Change existing routing tables to stop traffic from reaching the transaction server {Hard}
 2. Insert a false router on the communication line {Hard}
 3. Change address in the machine software to a false address {Hard}
 4. Physically destroy the communication line from the transaction server {Hard}
 5. Do a Distributed Denial-of-Service attack against the transaction server {Medium}
4. System acts unpredictable (OR) {Hard}
 1. Bad design of system {Hard}
 2. Bad programming of system {Hard}
 3. Staff user error {Hard}
5. Environmental disturbance (OR) {Hard}
 1. Electric disturbance {Hard}
 2. Electric interruption {Hard}
 3. Hardware failure {Hard}
 4. Telecommunications interruption {Hard}

10.3.5.1 Comparison

In this case, the attack trees look exactly the same and no advantage can be seen for either system. As the trees clearly shows, the easiest way to disrupt service is, as one might suspect, a DOS attack from the Internet. It is difficult to counter that attack but here resources would have to be spent in order to keep the server online in case of an attack.

10.3.6 Sabotage the service for a single customer

Sabotage the service for a customer in order to deny service to a specific customer resulting in a small loss of income for the company but a more serious inconvenience for the customer that might lead to the loss of the customer.

Constructed system {Easy}:

1. Modify the software for this customer(OR) {Easy}
 1. Trick the customer to install the fake software {Hard}
 2. Steal the mobile device to install the software and return the device {Hard}
 3. Borrow the mobile device to install the software and return the device {Easy}
2. Modify the transaction server to not give correct replies to this customer (OR) {Medium}
 1. Delete the customer account(OR) {Medium}
 1. Bribe/threaten/deceive one of the authorized staff {Medium}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
 2. Change the credit limit or the money spent on the attacked account(OR) {Medium}
 1. Bribe/threaten/deceive one of the authorized staff {Medium}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
 3. Change the PIN on the user account(OR) {Medium}
 1. Bribe/threaten/deceive one of the authorized staff {Medium}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
 4. Modify the software to not handle defined account number(OR) {Hard}
 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
3. Steal the mobile device {Hard}
4. Destroy the mobile device {Hard}
5. System acts unpredictable(OR) {Hard}
 1. Bad design of customer software {Hard}
 2. Bad programming of customer software {Hard}
 3. User error {Hard}
6. Environmental disturbance(OR) {Hard}
 1. Electrical interruption {Hard}
 2. Hardware failure {Hard}
 3. Telecommunications interruption {Hard}

Reference system {Medium}:

1. Modify the token for this customer(OR) {Hard}
 1. Steal the token to modify and return the token afterwards {Hard}
 2. Borrow the token to modify and return the token afterwards {Hard}
2. Modify the transaction server to not give correct replies to this customer (OR) {Medium}
 1. Delete the customer account(OR) {Medium}
 1. Bribe/threaten/deceive one of the authorized staff {Medium}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}
 2. Change the credit limit or the money spent on the attacked account(OR) {Medium}
 1. Bribe/threaten/deceive one of the authorized staff {Medium}
 2. Hack the transaction server {Hard}
 3. Be an authorized employee {Hard}

3. Change the PIN on the user account(OR){Medium}
 1. Bribe/threaten/deceive one of the authorized staff{Medium}
 2. Hack the transaction server{Hard}
 3. Be an authorized employee{Hard}
4. Modify the software to not handle defined account number(OR){Hard}
5. Bribe/threaten/deceive one of the authorized staff{Hard}
 1. Hack the transaction server{Hard}
 2. Be an authorized employee{Hard}
3. Steal the token{Hard}
4. Destroy the token{Hard}

10.3.6.1 Comparison

The attack trees show that it is easier to sabotage the service for a particular user if the user is responsible for the connection. This will easiest done by manipulating the software in the mobile phone. In the reference system, the easiest way would be to deviece someone in the personell that the account should be closed or the PIN changed for example so that the customer can not use the service.

10.3.7 Sabotage the supply service

This goal is used to sabotage the supply service in order to increase cost for the system, making it less profitable and eliminating one of the biggest gains by using a mobile payment system instead of cash. This might mean that the supply service has to service machines not needing service or that no message of service reaches the supply chain.

Constructed system {Easy}:

1. Modify the code from the machine(AND){Hard}
 1. Modify the input from the machine to the embedded system(OR){Hard}
 2. Modify the key so the result for the MCI value will be unreliable(AND){Hard}
 1. Aquire the key(OR){Hard}
 1. Bribe/threaten/decieve one of the authorized staff{Hard}
 2. Hack the transaction server{Hard}
 3. Be an authorized employee{Hard}
 2. Modify the key to give wrong values for MCI{Medium}
 3. Insert the new key in to the embedded system{Hard}
2. Modify the result on the transaction server(OR){Hard}
 1. Change the MCI value before it is evaluated(OR){Hard}
 1. Bribe/threaten/decieve one of the authorized staff{Hard}
 2. Hack the transaction server{Hard}
 3. Be an authorized employee{Hard}
 2. Modify the code in the machine status function to send wrong values(OR){Hard}
 1. Bribe/threaten/decieve one of the authorized staff{Hard}
 2. Hack the transaction server{Hard}
 3. Be an authorized employee{Hard}
3. Change the code to a random digit while transferring it(AND){Hard}
 1. Change MCI to random value{Medium}
 2. Change checksum to valid value{Hard}

Reference system {Hard}:

1. Modify the code from the machine(AND){Hard}
 1. Modify the input from the machine to the embedded system(OR){Hard}
 2. Modify the key so the result for the MCI value will be unreliable(AND){Hard}
 1. Acquire the key(OR){Hard}
 1. Bribe/threaten/deceive one of the authorized staff{Hard}

- 2. Hack the transaction server {Hard}
 - 3. Be an authorized employee {Hard}
- 2. Modify the key to give wrong values for MCI {Medium}
 - 3. Insert the new key in to the embedded system {Hard}
- 2. Modify the result on the transaction server (OR) {Hard}
 - 1. Change the MCI value before it is evaluated (OR) {Hard}
 - 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 - 2. Hack the transaction server {Hard}
 - 3. Be an authorized employee {Hard}
 - 2. Modify the code in the machine status function to send wrong values (OR) {Hard}
 - 1. Bribe/threaten/deceive one of the authorized staff {Hard}
 - 2. Hack the transaction server {Hard}
 - 3. Be an authorized employee {Hard}

10.3.7.1 Comparison

The attack trees show that it is hard to disturb the status messages to the transaction server when the customer can not control the communication between the machine and the server. However, when the customer controls the communication it is possible to change one digit for another, but the attacker has to know which digit to change and must fix the checksum again.

10.4 Attack tree comparison

The reference system has a slight advantage in the security aspect and should be considered more secure than the constructed system. However, the differences are not nearly big enough to warrant the extra security of installing an own connection for each machine, especially not considering the cost of doing so in comparison. It should also be noted that the reference system poses one threat that the constructed system does not have, it is connected to the Internet all the time and is therefore more vulnerable to automated attacks. The constructed system has very restricted communication to the machine which would be hard to attack.

11 DISCUSSION

The systems were compared in regards to the security aspects mentioned in chapter 6 by using the attack tree as a base for discussion. After discussing each aspect the research questions are answered in the summary.

11.1 Authentication

The constructed system uses a personal identification number in order to authenticate the buyer for each purchase which is a common method used in many systems. The PIN is kept secret by not being saved in the mobile device, except as a variable when the program is executing, and is never sent as plain text. In that regard, the constructed system has the same security level as other systems and as the reference system. However, when it comes to authenticating the seller, this is only really done when acquiring the identification towards the seller. After this, the seller is considered to be trusted by just keeping the same address.

By changing that address for a user, an attacker can redirect the user to another transaction server without the user being able to tell the difference. This requires the attacker to get the address changed in the mobile device of the user that is being attacked by either changing the address manually or by deceiving the user to install a program that modifies the address. However, in the reference system, this attack could possibly be done against the machine instead where the user does not have any control over the ability to manipulate the connection. The attack might be done by hacking the machine from the Internet in order to change the address or inserting a fake router into the connection that re-routes the traffic to another server. Either way, the user would not have any idea that the machine has been hacked and the information supplied instead goes to a fake transaction server. If the attacker uses this as a man-in-the-middle attack, neither the user nor the seller will be alerted of the problem. In the constructed system it would be easy to check that the server is correct by verifying the address in the mobile device against the real address.

To summarize, the constructed system is more vulnerable to an attack against a trusty user where as in the reference system it is harder to attack single users but it can be possible to attack the group of user using a particular machine. This conclusion can be generalized into other systems, if the possible way to modify the communication is in a machine that controls many users; that would be a larger threat than if each user is responsible for their own communication. Unless the attack could be automated, it would be more effective for an attacker to attack one target and get control of the data for many users instead of attacking each target separately.

11.2 Authorization

The constructed system does not offer any real differences in regards to authorization. Authorization is primary done one two conditions, that the item is available for sale and the money is available for payment. The payment system is not responsible for the physical order from the machine, this is handled by the machine and the system only authorize that that an order has been received from the machine and the status of the result from the transaction server. The authorization for the money can be done by the system depending on the implementation but in most cases there is some form of financial institute that authorizes the payments. If the payment method is done by pre-paid or post-paid, then the authorization will be done by the seller. However, this has no implications on the effects of relying on the connection of the customers only.

11.3 Availability

The main differences in availability between the constructed system and the reference system are the responsibility for this factor. In the reference system, the seller is responsible for

keeping a connection the whole way between the machines and the transaction server. This responsibility will probably be forwarded to the service provider for the connection. The responsibility might vary between implementations, depending on the used technologies, such as LAN, WLAN, GPRS or an ordinary phone connection. In the constructed system, the seller is only responsible for keeping the transaction server connected to the Internet, usually with help from the ISP.

The users are themselves responsible for providing the connection to the Internet with the use of their own MSP. The responsibilities for the company to keep the transaction server connected to the Internet as mentioned before, ensure that the machines are working correctly and verify that it is possible for the users to connect to their MSP from that point, i.e. the placement of the machine must be in a place that is covered by the MSP that the users wish to use. To summarize, this responsibility is shifted from the seller to the buyer in the constructed system in comparison to the reference system.

11.4 Confidentiality

Keeping the messages secret is the most important aspect when relying on an insecure connection through the user as any messages could easily be read by the users otherwise. Most communication methods, such as GSM and GPRS, have their own cryptographic solutions which are used regardless of the customer. When it comes to transferring the message to the machine however, only the Bluetooth method has a default encryption. In the constructed solution the message may also be read and altered in the mobile device, i.e. the user can control the communication while it passes the mobile device.

In the reference system, the connection is not directly accessible to the user and the seller might be able to rely on the message being encrypted between each node in the communication chain depending on the technologies chosen. In the constructed solution the message needs to be encrypted end-to-end, provided that the information has any value that needs to be held confidential. Even though this is not absolutely necessary to use this in the reference system, it is strongly recommended as it is impossible for the seller to have full control over the communication line. Using a connection not available to the user only lessens the risk that the attacker will read the communication; it does not remove it totally.

So to summarize this part, the communication between the machine and the user can easily be read on the constructed system while it is harder to read the communication that is forwarded to the transaction server. The same difficulty applies to the reference system also as no information is sent openly there. An important aspect of this is that on the constructed system, the seller is totally aware that all communication is read by the user and at least some of it can be read by the attacker. In the reference system, it might be easy to assume that it would be too hard for the attacker to read the communication and by that be over-confident in the security of the system.

The cryptography is another aspect to this field, how the messages are encrypted. Both systems have the same constraints on memory and processing power in the machine. This makes the encryption and decryption of the codes slower and it might be necessary to use a less complicated algorithm. This difference between the systems is the amount of data that can be sent, the reference system could for example use negotiated session keys for encryption while the constructed system is forced to rely on a pre-shared key. The constructed system also has another disadvantage, the processing power of mobile devices is often very low and only a few can use SSL for example. This makes it hard to encrypt the PIN for that user with a good level of security. The message is in both systems encrypted from end-to-end, but in the constructed system, the PIN is added to the message.

In the aspect of confidentiality, the reference system has a clear advantage and can be considered as a more secure solution.

11.5 Integrity

Based on the conclusions from the confidentiality section, the systems need a method for guaranteeing the integrity of the messages. This has been implemented as checksums that are added before encrypting the messages. The integrity aspect is especially important in the constructed solution as this has such open communication that could easily be modified. If the positions of each character in the encrypted messages remain the same it could otherwise be possible to modify the message to supply a modified amount. Note that the encryption would still keep the amount secret but it could still be changed and if the order is for the maximum credit, a change of this value would result in a lower cost. This proves the importance of verifying the integrity of each message. The messages should always be checked for integrity, even if it is considered highly unlikely that the communication has been modified.

This is covered in the Canadian article but the author focuses on it as a safety issue because they assume that a possible error would be because of hardware or user error [3]. This is good to cover but it does not give the whole picture as it disregards the attacker that will actively seek for a security hole. The same article also mentions another aspect that can be important to keep in mind when designing the integrity check; the length of the message. The system specified there uses IrDA as a primary transfer method but uses keypad as a backup method. When using keypad, it is critical to keep the number of characters to enter as low as possible to make the system easy to use for the customers. Therefore, the integrity control should use as few characters as possible. If the transfer method allows longer messages this is no longer such an important aspect.

In short, integrity is equally important for both the reference system and the constructed system but the constructed system would be more easily attacked without a valid integrity check for messages. The reference system here has the advantage of being able to send more information than the user of the constructed system might be willing to do as the traffic cost money. It can therefore use more characters for integrity checks of each message.

11.6 Non-repudiation

The binding of the customer to the purchase is highly dependant on the functionality of the confidentiality and the integrity that insures that only the user could have made the purchases. If this can not be guaranteed, the non-repudiation function of the system will cease to work. There is also another aspect regarding vending machines as the seller is an automated function it can not physically prove that the item has been delivered. Therefore, it would be more believable for the attacker to call customer service and claim that the item was never delivered than claiming that the purchase was made by an attacker.

The reference system is here considered to have the same implementation as the constructed system except for the communication method but as the communication here do not have the same limitations as the constructed system this problem could be solved for this system. This could be done by sensors in the machine that rapport to the transaction server whenever an item has been purchased. So to summarize, this aspect depends highly on other aspects but the reference system has the advantage of free data communication that could be used for better control.

11.7 Privacy

This concerns the systems primarily as the difficulty of gathering information as it is sent and the difficulty of interpreting it. Therefore it is highly dependant on the confidentiality,

both as the availability to communication and as the readability of the communication. If the cryptography can be broken, the messages can be read and information can be gathered. The gathering of this information is the key in this aspect; the most information will be gathered by reading the traffic at the transaction server as this will give information about all customers and all purchases.

On the reference system, the communication will always be from the machines and all data will be encrypted. Therefore, assuming the confidentiality to be secure, the only information that can be gathered from this is when a purchase was made at what machine. On the constructed system however, the information will also include the address of the user. This system will therefore allow for pinpointing the location of users at certain times.

The other place to gather information is at the machines, monitoring the communication between that specific machine and the transaction server in the reference system or monitoring the information that is entered in the machine on both systems. The reference system will here give the same information as mentioned earlier but from only this machine. Using fake hardware or monitoring equipment to monitor the input to the machines will on this system give information about the user, as time, place and order placed. Using the same method on the constructed system will however not reveal any information about the user, only what was purchased when.

So both systems has their advantages and disadvantages in this aspect but as it easier to control that no one can read the communication at the transaction server than controlling all machines, the constructed system gives a better level of security against privacy issues. This is based on that is harder to gain the information on where each customer has been by monitoring the transaction server than the machines that are often publicly available.

11.8 Reliability

A machine that is out of order will be noticeable immediately on the reference system while it on the constructed system will not be noticed until someone reports it to be broken or the maintenance staff finds it. The reference system here has the advantage of considerable shorter downtime. It can also report the contents of the machine in real-time to the transaction server in order to keep all items available. A disadvantage against this system is the dependency on one singular connection, if this is broken or attacked this would make the machine useless until the conditions change. It could, for example, easily be attacked by a DOS attack from the Internet. The constructed system however uses different connections for each user, making it impossible to execute a DOS attack at a distance. Both systems are however susceptible to a direct DOS attack as broken displays or input devices.

The term reliability also includes that neither side should lose anything if the purchase is interrupted. In the constructed system, this is harder to achieve as the communication ends when the user has the code needed for the purchase. This does not guarantee that the user has received the purchased item, only the code. The reference system however can wait until the item has been delivered to finish the transaction and allow the transaction server to withdraw the money. The constructed system could however use the next connection to send a verification that the previous purchase was completed but this is unreliable and the control will always be as a refund as the purchase has already been completed.

Both systems present weaknesses and no system can be claimed to have the direct advantage when it comes to reliability.

11.9 Advantages of constructed system

The system can as most payment systems also be used in a wide area of applications, just not vending machines but also parking fees and magazine stands for example. The only requirements are electricity and that the users can get a connection to their MSP.

Maybe the largest advantage of this sort of system, in difference to other mobile payment systems, is the cost efficiency. The cost of implementing the system will be lower than using the reference system as the embedded system lacks any long range communication hardware and the machines does not need their own connection. The reference system has the cost of the connection that adds an extra cost to each transaction and/or a constant cost for keeping the connection available.

As all communication is sent through the user's mobile device, it can also be used to view previous purchases. This was mentioned as one of the key issues in making mobile payments easier to use, together with a wide array of uses for the system, in a Norwegian study [12]. This fact also provides the benefit of making DOS attacks from a distance impossible.

11.10 Disadvantages of constructed system

The largest disadvantage of the constructed system in comparison to the reference system is the limitations on data transfer. It puts restrictions on, for example, the feedback data to the supply chain and the key management. This is however necessary as long as the communication can not be guaranteed to be cost-free for the users of the system.

The system also suffers from the low processing power of it's componets, primarily the mobile devices, which makes it hard to insert a PIN to the message without making the PIN readable to anyone that can monitor the communication as the system must rely on less advanced cryptographic algorithms.

11.11 Effects of combining the two systems

One of the motivations for the project was to check if using the constructed system as a backup system would reduce the threat to the communication line. Using the reference system as a primary method for payment and the constructed system as a backup method would help limit this threat as the customers can chose to use their own connections instead if the main communication line has failed for any reason. However, some of the threats are not helped when combining the systems and the result can be summarized in regards to the eight security aspects.

When it comes to authentication, combining the two systems gives only negative results as it is now easy to gain information about specific accounts by either monitoring their mobile device or by monitor one of their used machines. Instead of having one way of attacking specific accounts, the attacker can now use two methods for greater success. Authorization is not affected. Availability is the greatest gain from combining the two methods as the customers now has two seperate methods for performing the purchase and it is highly unlikely that both would fail at the same time. The confidentiality aspect of the combined system has the same limitation as using the two systems as separate, the limitations are still the same and no combined effect can be found.

Integrity can use the combined methods to verify the correctness of each message but it might be more work than it is worth. One large benifit of the combined system is that the non-repudiation aspect can be controlled very efficiently, using the reference system to verify all successful payments, even those done by the constructed system when the reference system has not been available. Sadly, privacy has the same issues as authentication, it just opens up for attacks on both systems and makes it easier for the

attacker. Reliability is only affected in a positive way, keeping the system more available and more precise than either of the two systems used separately.

So to summarize, using the two systems as a combined system would result positively in regards to service issues, it is more available to the customer and the machines can be controlled in a better way. However, the system is also more easily attacked, allowing for both the attack methods of the two systems to attack authentication and privacy.

11.12 Summary

Evaluating the result from the discussion and the attack tree of the proposed system shows that it is as in most cases the human factor that is the weak point in the security. Should the attacker use social engineering to borrow the mobile device of the target, it would probably result in easy access to modify the software. However, setting up restrictions on the legitimate usage of the system reduces the financial gain to very small unless the attacker can acquire an account open for transactions for a longer period. This might actually be the weakest point with this sort of system, if the account identification number and the personal identification number are known and can be used by an attacker, the customer might lose respect for the company and find someone else with a solution that is harder to attack. Making the account information more difficult to extract would make it harder to steal another person's account and diminish the differences in security between the two systems.

The proposed system actually has an advantage here as a mobile device is often used and would be missed if stolen rather quickly while a token used solely for buying items from vending machines might not be used that often and therefore be of use for longer time. Based on the attack trees of the two systems, there is no difference in security that is large enough to be able to say that the proposed system can not be considered safe in comparison to the reference system. As proven by the attack trees, the easiest way to get a free soda is to just call customer service and complain that the item never was delivered from the machine. So the weakest point in the system is the human factor. The damages in that case are however small and with education, larger effects can be avoided by informing the staff on social engineering attacks so that no valuable information is leaked.

As shown by the discussion on availability, a larger part of the security is transferred from the seller to the buyer as the user now gets the responsibility for making the purchases possible. The discussion on authentication also shows that the easiest target to attack are the users and as seen in the non-repudiation discussion, some of the security of the purchases is now dependant on customer trust. This shows that more of the security is moved from the seller to customer in comparison to a regular mobile payment system such as the reference system. Combine this with the results from the attack trees and the human factor can be concluded to present one of the biggest threats against this system.

The confidentiality and integrity discussions show that the technological security of the constructed system is more susceptible for an attack than that of the reference system. However, the security of the constructed system is made difficult enough to dissuade the occasional attacker but might not prove secure enough to the professional attacker. But for the value in the system, the effort must be considered larger than the gain of a successful attack. For example, the discussions on confidentiality and privacy show that there is not much usable information that can be read by the attacker studying the communication between the machine and the user.

It is however easy to gather the information between a machine and its users but that does not consist of any user data that could be used to use someone else's account. In order to get free items that leaves the attacker with the choice of attacking the user or attacking the

cryptography of the system in order to verify an order without contacting the transaction server. With this choice, the user is probably an easier target.

In answer to the first research question; the information presented in this discussion and the attack trees indicates that the constructed system can not be considered as secure as the reference system. This conclusion has been reached based on that the reference system being more secure in confidentiality and can provide a higher level of integrity to the messages which leads to the non-repudiation aspect being more secure. When it comes to privacy, authentication and availability the constructed system has the advantage. However, the system security depends more on the confidentiality and the integrity of the messages. The attack tree also shows that the constructed system is slightly more susceptible for an attack.

Regarding the second research question, this is partly answered by the motivation for the answer on the first question. A larger part of the security is transferred from the seller to the buyer as the user now gets the responsibility for making the purchases possible as shown in the discussion about availability. The discussion on authentication also shows that it is easiest target to attack are the user and they are also the greatest threat against privacy as shown in the attack tree. This is also supported by the literature, for example, Kevin Mitnicks book "The art of Deception"[XXX]. The attack trees also shows that the easiest way of getting free items is to call customer service and claim that the item was never delivered. This is one of the key issues with this system; the seller is automated and can not prove that what was purchased has been delivered as discussed in the non-repudiation section. The other key issue is the confidentiality of the system because the messages are easily read while transferred which gives the attacker access to as much data that can be gathered. This combined with the limitations in processing power on embedded systems and the constraints on key handling presents a problem a large threat. The complete list of threats can be found in the attack tree but the human factor must however be considered as the largest threat against this system as people generally trusts each other.

The third question is somewhat subjective as to what is considered secure enough but all the threats against the constructed system can be handled, either by countermeasures or by risk acceptance. The security of the constructed system must be weighed against the value of the attacks. As shown in the attack tree, the critical goals are hard to achieve but small goals as getting a free item can be achieved easily. These losses are however easily controlled as it is highly unlikely that one specific customer does not get the purchased items in any significant higher amount of times than the general customer base. Using a restriction on the amount the customers are able to spend on a period of time also makes a successful attack of less value. So considering the attack tree and the discussion, the effort of an attack must be deemed much larger than the gain.

As mentioned in the advantages section, the perhaps biggest advantage of the constructed system is that the connection can be transferred to the buyer. This would cut much of the cost of implementing the service and existing vending machines could be equipped with a electronic payment module in combination with the ordinary payment method.

12 CONCLUSION

The conclusions drawn from this work is that the connection can be shifted from the seller to the buyer but will result in a shift of threats and the security can not be kept at the same level. The difference in security is however not that large that it would warrant the additional cost of keeping a connection for each machine. A shift in the attack point can be seen with this system where the most cost effective attack is moved from the seller to the buyer as there is no easy way to get access to the total communication between the transaction server and all users. The studied method displays larger threats against confidentiality, integrity and non-repudiation while it better handles availability, authentication and privacy.

Deceiving the customer to give valuable information would present the most cost-effective way to attack the system. Therefore it is important that the consumers of today's society is aware of the threats against them and uses common sense and exercise caution when being subjected to an attack. This is not new for the system evaluated in this thesis; most systems are vulnerable to social engineering. It does however present a problem for the seller when the security is moved from the seller to the buyer, the buyer might not be willing to accept a larger responsibility for the security and the seller will then be forced to accept the threats and compensate any customers that has been deceived or risk losing the customer to another service provider.

Combining the two systems would result in a system with very positive impacts on reliability, non-repudiation and availability. However, the system would also suffer from both an attacker given the chance to attack the system using both the methods from the constructed system and the reference system in regards to authentication, confidentiality and privacy.

To conclude, the threats against the method of using the customers connection are somewhat larger than against the traditional method but mainly it just displays different weaknesses. However, if one were to seek a solution that better handles identity thefts and Denial of Service attacks, this might be the method of choice.

13 FURTHER WORK

Based on the experiences drawn from researching risk and threat analysis on mobile electronic payment systems, this is an area that needs to be further investigated. There is next to no documentation available regarding the security of such systems as discussed in this thesis. There is also a lack of a platform used to compare the security of similar concepts which would be useful in order to evaluate different technologies. This might however depend on the difficulty of quantifying security which is highly subjective and can only be used as a pointer towards a correct value.

14 REFERENCES

- [1] R. Andersson, "Security engineering: a guide to building dependable distributed systems", Wiley Computer Publishing (2001)
- [2] N. Asokan, P.A Janson, "*The state of the art in electronic payment systems*", IEEE Computer Journal Vol. 30 No. 9, p 28-35 (1997)
- [3] S.B.Z Azami, M. Tanabian, "*Automatic mobile payment on a non-connected vending machine*", Electrical and Computer Engineering, 2004. Canadian Conference on, Vol. 2 , p. 731-734(2004)
- [4] S.B.Z Azami, M. Tanabian, "*Modeling the customer behavior in the mobile payment on a non-connected vending machine*", Electrical and Computer Engineering, 2004. Canadian Conference on, Vol. 2, p. 815-818(2004)
- [5] G. Bjåen, "*Security in GPRS*", Master Thesis, Agder University College, Norway (2001)
- [6] J.W. Creswell, "Research design: Qualitative, quantitative, and mixed method approaches", Sage Publications Inc. (2003)
- [7] A. Dennis, "*Classification and Characteristics of Electronic Payment Systems*", Electronic Commerce and Web technologies, Second International Conference on (2002)
- [8] J. Gustafsson, "*Pki-Security In Mobile Business – Case: Sonera Smartrust*", <http://citeseer.ist.psu.edu/466933.html> (2000)
- [9] A. Herzberg, "*Payments and banking with mobile personal devices*", Communications of the ACM (2003)
- [10] I. John, D.K Angleos, "*Offline micropayments without trusted hardware*" Proceedings of the Fifth International Conference on Financial Cryptography (2002)
- [11] A. Kini, "*Trust in Electronic Commerce: Definition and Theoretical Considerations*", hicc, p. 0051 (1998)
- [12] S. Kristoffersen, A. Synstad, K. Sorli, "*What do users think of mobile payment?*", <http://folk.uio.no/steinkri/Papers/isoneworld.pdf> (2005)
- [13] E. Ohbuchi, "*Barcode readers using the camera device in mobile phones*", Cyberworlds, 2004 International Conference on (2004)
- [14] T. Peltier, "*Information Security Risk Analysis*", Boca Raton: Auerbach 2 ed. (2005)
- [15] J. Rautpolo, "*GPRS Security - Secure Remote Connections over GPRS*", Technical University of Helsinki, Department of Computer Science (2000)
- [16] C. Robson, "Real world research: a resource for social scientists and practitioner - researchers", Blackwell publishing(2002)
- [17] B. Schneier, "*Attack Trees – Modelling security threats*", Dr. Dobb's Journal, <http://www.schneier.com/paper-attacktrees-ddj-ft.html> (1999)

- [18] B.Schneier, "Secret and lies: Digital security in a networked world", John Wiley & Sons (2004)
- [19] S. Schwiderski-Grosche, H. Knospe, "*Secure mobile commerce*", Electronics & Communication Engineering Journal Vol. 14 No. 5, p.228-238 (2002)
- [20] S. Srinivasan, "*Role of trust in e-business success*", Information Management and Computer Security, Vol. 12 No. 1, p. 66-72 (2004)
- [21] U. Varshney, "*Mobile Payments*", IEEE Computer Journal Vol. 35 No. 12, p. 120-121(2002)
- [22] C. Xenakis, "*Malicious actions against the GPRS technology*", Journal in Computer Virology (2006)
- [23] Z. Xiaolin, C. Deren, "*Study of mobile payments system*", E-Commerce, 2003. CEC 2003, IEEE International conference on, p. 24-27 (2003)
- [24] P. Yousef, "*GSM-Security A Survey and Evaluation of the Current Situation*", Master's thesis, Linkoping Institute of Technology (2004)
- [25] "*Dial-a-coke*", http://telephonyonline.com/wireless/mag/wireless_dialacoke/