KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES

Information security analysis for remotely served customer service concept

Zheng Shutao

Bachelor's thesis of the Degree Programme in Business Information Technology

Bachelor of Business Administration (BBA)

TORNIO 2012

ABSTRACT

Zheng, Shutao 2012. Information security analysis for remotely served customer service concept. Bachelor’s Thesis. Kemi-Tornio University of Applied Sciences. Business and Culture. Pages 50.

In today’s global business environment, the importance of information has been widely accepted. Information is widely used for commercial and governmental organizations’ information systems. Besides, there are an increasing number of commercial and governmental organizations depending on information. However, as for the risks of operational business, benefits and opportunities, they are making information security management an increasingly critical part of business management.

This thesis work is a case study of a network kiosk. The objective of this thesis is to analyze what the information security risks are in this system, what the physical threats, the technical threats or malfunctions, and the communication and software threats are. This thesis focuses on how to improve the system of information security.

Constructive research is a core research methodology which covers this research work to accomplish the objective of the thesis work. The data was collected from scientific resources from libraries and from a personal interview with the CEO of ETA Company. Besides, other data sources used for this thesis are the formal PDF documents and E-Books found through Web searching.

The expected output of this thesis is an analysis of the threats in the kiosk system. This research provides suggestions to improve the security systems for the case company called ETA Company. This research also gives guidelines for further development to build a table and reliable security architecture for remotely served customer service concept.

Keywords: Kiosk, Audible visual alarm, VPN, Smart card, DDoS, RAID

ABBREVIATIONS

A/V	Audio/Video (hereinafter A/V)
ACK	Acknowledgement (hereinafter ACK)
ADSL	Asymmetric Digital Subscriber Line (hereinafter ADSL)
ATM	Automatic Teller Machine (hereinafter ATM)
B2C	Business to Customer (hereinafter B2C)
CERT	Computer Emergency Response Team
CC	Coordination Center (hereinafter CERT/CC)
CPU	Central Processing Unit (hereinafter CPU)
CRM	Customer Relationship Management (hereinafter CRM)
DoS	Denial of Service (hereinafter DoS)
DDoS	Distributed Denial of Service (hereinafter DDoS)
DVR	Digital Video Record (hereinafter DVR)
ETA	Etapalveluteknikka (hereinafter ETA)
FAT	File Allocation Table (hereinafter FAT)
NTFS	New Technology File System (hereinafter NTFS)
RAID	Redundant Array of Independent Disks (hereinafter RAID)
RST	Reset (hereinafter RST)
SYN	Synchronize (hereinafter SYN)
UPS	Uninterrupted Power Supply (hereinafter UPS)
VAIO	Video Audio Integrated Operation (hereinafter VAIO)
VPN	Virtual Private Network (hereinafter VPN)

FIGURES

PICTURES

TABLES

1 INTRODUCTION

1.1 Motivation and background

Information security is not only a traditional sense of security, which is adding a simple device such as a firewall or a router. However, also as a guarantee of information security of the system, it should be a system and an overall concept. “Information security is to make information systems avoid a series of threats to ensure the continuity of business, to minimize the loss of business so as to maximize the return of investment and business” (Information Security Plan 2011).

The definition of information security is mainly reflected in the following three aspects: they are confidentiality, integrity and availability. In the confidentiality part, it is to ensure the information only allowing authorized access. In the integrity part, it is to ensure the information protection and processing methods are accurate and complete. In the availability part, it is to ensure it can get access to the information and the corresponding assets when the authorizer needs it.

At present, the network security environment is facing a new challenge. The security technology in the separate network has many limitations, facing increasingly complex and frequent hacker attacks, garbage intrusion and all kinds of Internet fraud crime behavior. The most common network security incidents are network attacks and malicious code attacks. “Network attacks use the tools and technology to attack and invade the network information system, such as network detection and information collection, vulnerabilities detection, sniffer to get account, and password and authority in an illegal way” (DeepSearcher 2012). In addition, the user identity theft and fraud is another challenge, such as stealing and destroying user or business data, or controlling and destroying the system operation. “For making malicious code attacks program code is used which deliberately executes malicious tasks in the computer. The most common network security incidents are viruses, Trojan horses, worms, the trapdoor, spyware, and eavesdropping on software.” (Lin 2009).

Because of an increasing popularity of self-service terminals, the network kiosk system creates a lot of benefits between commercial applications and consumer. These benefits include the ease of use and autonomy, reduced transaction time and staffing, in addition to extended time of service without having restrictions of place. All aspects above are traditional business model which cannot be achieved. Therefore, the self-service terminal is an important innovation and breakthrough in this new business model discussed further below and illustrated in Figure 1 below.

The disadvantages of traditional business model have become increasingly evident. However, the self-help service is gradually replacing the traditional face to face type of service. In comparison with the traditional business model, the self-help service has advantages. Figure 1 illustrates the multiple channels of business models (EVT Solutions 2009), Compared with the retail stores, the kiosk system can save the cost but provide the same quality of service. The clients do not have to spend a lot of money on rent an office or a shop for their business as well. Compared with the on-line shop, the kiosk system is easy to use, because users do not need to master the computer knowledge. Compared with the phone orders, the advantage of the kiosk system is to provide the images, since users could have a visual impression when they select products. In addition, the kiosk system realizes seven days a week, 24hours a day of continuous service. Therefore, an increasing number of people will pay attention to this new type of remotely served customer service concept.

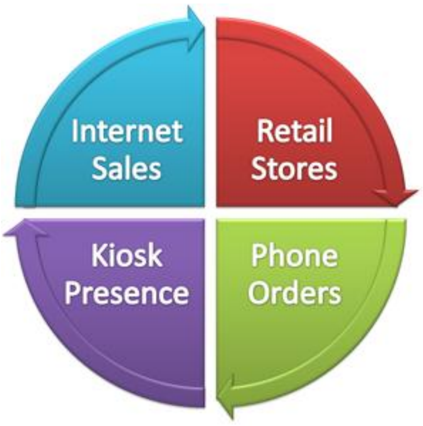


Figure 1. Multiple channels of business models (EVT Solutions 2009)

Through a virtual service desk the self-service machine can provide self-service. “This self-service includes face to face interaction with the customer, as well as the delivery and reception of objects and documents, such as key preserving, receipts, forms to fill in and sign, handling payment and signing documents” (Face2Face 2010, Start.) Further, other similar functions that may be necessary can be adapted as required. It provides a high quality actual interaction between customers and service staff.

ETA Company as a new company in this industry, they plan to build a new background office platform as a service supplier which provides the call center service, cooperating with a self-service machine company as a support office which provides the main function requirement. This company combines both advantages to carry out their own business model.

Different from other information kiosks on the market, the case company uses an interactive system. There is a service attendant in the back office that provides real time communication with the customer by VAIO. This Virtual Service Desk allows any service as provided by a real person, “such as providing answers to inquiries in a face-to-face setting via audio-visual technique, providing advice and the ability to handle check-in and check-out paperwork, such as copying passports, providing forms and receiving these forms filled in and signed, handling out and collecting door keys, and exchanging receipts and payment” (Face2Face 2010, Start.)

Currently, this company is mainly engaged in the business of booking tickets, booking hotels and commodity exhibition and sales through the kiosk. However, they plan to use the kiosk instead of traditional government office in the near future. As a result, users can handle any business they need by the remote self-service terminal. Because increasingly sensitive information will be collected by the kiosk, the security of the kiosk system needs to further increase.

In terms of the security system level of the network kiosk, it completely depends on the customers who rent the network kiosk. That means if customer has a perfect security system, the network kiosk has a strong security system as well. Unfortunately, the ETA

Company is a new company which is just starting their business. Their security system is not perfect either. This thesis is providing some suggestions to improve the security system for ETA Company. This thesis work is made for both the kiosk machine and their back office, analyzing what the risks of the system are and giving some suggestions for improving the security system.

In this thesis collect data through interviews and ask questions about the structure of the kiosk system by email from the CEO of ETA Company, in order to understand the business model of this case company. On the basis of the data collected, the composition and structure of the entire system are analyzed to identify the possible security risks, from the following three aspects: physical threats, technical threats or malfunctions, and communication and software threats. Following the analysis stage, corresponding solutions for the sake of avoiding the risks are suggested for improving the security of the network kiosk system. The method used to find the solution is reading widely established material in order to collect useful information, and in addition, to provide the thesis author’s own views and combine the views with the opinions from his supervisor and top leadership of ETA Company. The ultimate aim is to analyze what the information security risks are in kiosk system and put forward a set of feasible and effective suggestions for improvement.

1.2 The structure of my thesis

The subsequent chapters are divided into five chapters. The second chapter introduces the research process, containing the description of the research topic and question, researches methodology and expected the output of this treatise? The third chapter is about the presentation of the kiosk system. Chapter three respectively introduces the effects and advantages of the kiosk system. Moreover, the special functions mentioned which can be provided by the kiosk system and the structure of kiosk system.

Chapter four focuses on the risk analysis for the kiosk system. The risks of the kiosk system are discussed from the following points of view: the risks from physical safety, the risks from technical threats or malfunction, and the risks from communication and software threats. Chapter five is to put forward the author’s own suggestions to improve the information security of the kiosk system. The suggestions include combining an audible and visual alarm into the kiosk device, establishing a VPN to connect to remotely users and business partners, and encrypting and decrypting by a smart card. Chapter six shows the results of this thesis, the self evaluation of the author’s work and the suggestions for further research.

2 RESEARCH PROCESS

2.1 Research topic and questions

My thesis topic is “information security analysis for remotely served customer service concept”. The remotely served customer service concept provides a high quality actual interaction between customers and the staffs of back office. In comparison with the traditional business model, the main advantage of remotely served customer concept is that it combines both advantages of traditional business and online business. This concept is not only saving the expenses for the factory but also bringing the convenience to the users. Improved the cost effectiveness and achieved a kind of uninterrupted service.

Kiosk is one type of the remotely served customer service concept. It is widely used in service providers, information support centers and all kind of rental or booking stations. Furthermore, it is a win-win concept for the company and their business partners, the kiosk will make better business for them. For the customer, the kiosk will improve the quality of service and easier handling of customer’s diverse needs.

Because the advantages of the mentioned above, with improving utilization rate of network kiosk system, while it is increasing the risk of being attacked from hackers. The objective of this research is to define the security issues for their network kiosk system, Analysis each link might be attacked and estimate their risks. All the information collected through the constructive research, combined with the author suggestions and advice from experts, put forward a solution to improving the security system of network kiosk.

This thesis is to analysis the risk of security system for this company, and combines their development trend and speculates the requirements they need to get the frame structure of security system in the future, put forward a scheme to improve their security system.

RQ1. What is the information security risk from physical threats?
After the functional analysis, for the kiosk machine there is a physical attack from human malicious damage. For example, some vandals' want to steal the hardware of the kiosk, "due to the kiosk could be placed in the middle of mall or even in an airport." (Smith 2008), Users operate it on their own, mostly without staff supervision or intervention. Thus, the suggestion of solution is to start from use of the alarm device.

RQ2. What is the information security risk from technical threats or malfunctions?
The information security risks from technical threats are relevant computer viruses, hackers attack and denial of service attacks. For instance, assume a scenario when user using a kiosk to rent a car, after the user complete the correct operation by the accordance with the instructions from the kiosk attendant. However, the cabinet of the key storage is still closed. Or imagine another picture, vandals' attack the back office and control the kiosk, making the cabinet of the key storage open without any normal operation. Another the malfunctions happened in the kiosk device, such as printer or credit card reader. Moreover, when power failure in the middle of a transaction. Therefore, the author should consider how to avoid such a kind of things happening. Besides, there is a database in the back office which stores a large number of sensitive data as well. Therefore, considering this solution is the start from establishes high level security network and improves the system management.

RQ3. What is the information security risk from communication and software threats?
If information safety risk caused by software problems, there should be a functional deficiency of firewall is easy to invade. In addition, depending on the applications and data requirements, the back office is often connected to a network. The sensitive data will become the target of hackers. "According to statistics, at present 70% attack is to happen in the application layer but network layer." (Desmond 2004) To this kind of attack, the protective effect of traditional network firewall is unsatisfactory. Consequently, to solve this problem needs a tool to encrypt and decrypt the date before transmission. In addition, data recovery also needs to be considered.

2.2 Research Methodology

“The Constructive research approach is to build an artifact to solve a specific problem, in order to produce knowledge concerning how the problem can be solved, and if previous solutions exist, how to create a new solution or better than old. The constructive approach means problem solving through the construction of models, charts, plans or groups.” (Kasanen & Lukka & Siitonen 1993, 243-263)

2.2.1 Research method

Constructive research is a core research methodology covering my research work. Therefore I should follow every phase of constructive research. The first step during the constructive research is to get one topic after discussing with my supervisor and the CEO of ETA Company. Then, after confirming my thesis topic is information security analysis for remotely served customer service concept, I should scan lots of relevant literature about network kiosk system and information security. To get a big picture of existing knowledge, this includes two aspects. One is the existing system security structure analysis, trying to detect the threats and the places need to improve. Another is requirements of the theory and technology to construct a good information security system. Next the author will unceasingly proposing the new suggestions and verify the feasibility of it. Finally, give the rational suggestions to improve the security system for ETA Company. (Kasanen & Lukka & Siitonen 1993, 243-263) In addition, the author hopes this thesis can provide a guideline for other companies which want to build their own security system.

2.2.2 Collection and analysis of data

Data collection and analysis are important aspects of my research work. The author collects and read some relevant materials or information sources, in order to construct a set of practical information security system. In data collection, the data availability and usefulness are the very important reference to guarantee the scientific of resources. “The quality of data refers to their accuracy, reliability and completeness” (Krishnaswami &

Satyaprasad 2010, 94). Therefore, the author prefers to collect the resources coming from libraries and personal interview with the CEO of ETA Company. Besides, other small parts of collections are the formal PDF documents and E-Books from Web searching.

“What you’ll end up with after using inferential statistics is a probability estimate” (Rugg 2008, 72). I use inferential statistics to get probability of the results, that a phenomenon difference between groups is a trustworthy one or one that might have occurred by opportunity in this research. Thus, the first step of my research analysis is to risk management of network kiosk system. The next step is to analysis what should be a viable construct composition of the security system. The final step is to analysis the feasibility of the security system with the method of hypothesis.

“Structured in-person interviews can be useful when participants may have difficulty with a written survey or when the researcher wants to be able to ask clarifying or probing questions in addition to structured questions” (Johnson 2002, 90). The author collection information and data by interview or ask questions by email from the CEO of ETA Company. Collection specific information and data about what is the structure of the system and what kind of security system does this company already have. Furthermore, ask questions from the customer by survey, trying to understand what will be the development tendency of the network kiosk system. In order to know what will be the security requirements of the network kiosk system.

2.3 Expected output

The expected output of this thesis is containing two parts. Firstly, the author lists each risks and threats of kiosk system after research. Secondly, the author will puts forward some solutions to improve their security system for this network kiosk company. The achievement will be manifested in the following respects.

The objective of this thesis is to analyze what the information security risks are in this system, what the physical threats, the technical threats or malfunctions and the communication and software threats are.

Then, the thesis will focus on how to improve the system of information security. The author considers the deficiencies of this security system and lists them out. List the proper security architecture for this network kiosk system in the author’s opinion, which one can provide the active protection before being attacked, defense during the attacked and data recovery after being attacked. Finally, ask for help from experts and literature to demonstrate and modify the author own thought. The author will put forward a final solution to improve security system for this network kiosk company.

“This network mapping should be maintained and updated any time the network is modified” (SANS 2003, 9.) This solution is to improve the network kiosk security platform, while the administrators are able to implement both security deployment and configuration for their robust network. It can use a unified control platform to comprehend defense current network threats, supply the existing safety technology of network product. This is also in the most cost effective, to implement controls more network security function, and without loss of network availability and normal operation time.

3 FACE2FACE KIOSK SYSTEM

3.1 Face2face kiosk

Kiosks are one possible solution for providing services remotely. The remote service is an individual electronic computer terminal that allows the consumer to access information and also accomplishes various kinds of feasible transactions, such as renting a car or booking train tickets, booking hotels or reserving theater tickets. This is a new type of face-to-face customer service kiosk. The service utilizes a remote audio and video connection to provide the users to have a communication with a customer attendant who can help users meet their needs.

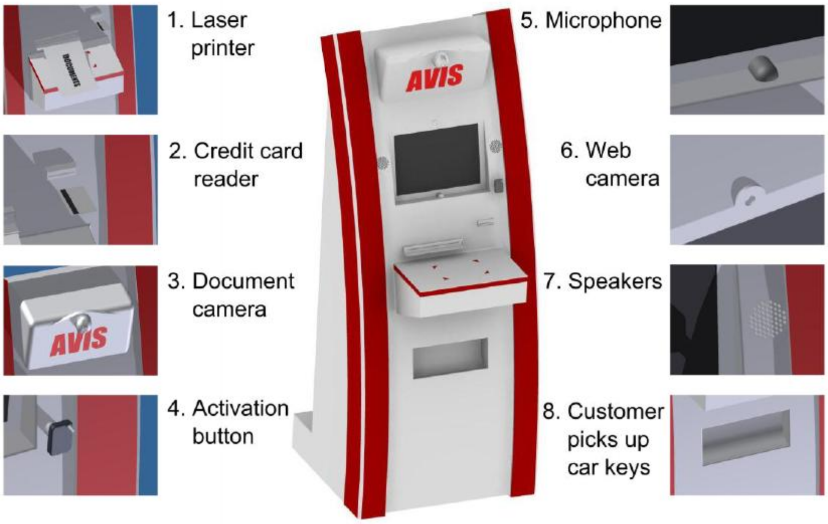
In addition, the kiosk service is to provide a solution that one can deliver personal customer service with remote work, which makes customers experience the customer service as a Face-to-Face phenomenon, and supplies the same flexibility and possibility to serve the customer as in a traditional way of serving. This system not only decreases the utilization rate of employees, but also saves the expenses and expands the company's operations and services. (Face2Face 2010, Start)

Take AVIS kiosk is an example. When users press the activation button, the self service of car rental begins at the same time, creating communication between the car renter and the attendant of the kiosk by the cooperation via the microphone, web camera and speakers. After the attendants understands what kinds of service the renter wants via this kind of face to face communication, the kiosk attendant will help the renter complete the formalities of the lease step by step. For example, after the renter determines the make and model of the car, the kiosk attendant will guide the renter in how to put both sides of his driving license under the document camera and slot the credit card via the credit card reader. After this stage is completed the attendant of the kiosk will receive the reservation. The renter will get the rental contract from the laser printer at the same time. The kiosk attendant will request the renter to sign the contract. The next stage involves teaching the renter to put the contract into the document scanner, which is hidden beneath the platform. After completing all the above operations, the renter can pick up the key from an assigned place. (Avis Rent A Car System 2012)

The first advantage is a face-to-face kiosk device, which can provide human interaction service through audio and video technology. The technology not only makes customers and attendants see and hear each other in real-time, but it also offers more intuitive impression when demonstrating products for the customers. The second advantage of this kiosk device is that it can provide multiple remotely controlled functions, i.e. it can provide the remote control to open the cabinet, after which the renter can get the auto key. The third advantage of this kiosk machine is the one-to-many operation. One customer-service representative can provide service for several kiosks. This solution is undoubtedly reducing the amount of labor used. Another advantage of the kiosk device is to reduce the cost to set up a shop, as the kiosk could provide the same quality of service but the cost is much lower than setting up a shop. In addition, it can provide 24 hours a day uninterrupted service. The next advantage of the kiosk machine is that it can provide a platform to many companies, and they can put the advertisement into the kiosk device. It affords a second way for their profits. The last advantage of kiosk machine is it has UPS to avoid the power failure during the transactions, if customer wants to secure transactions, after power failure the kiosk starts automatically and keeping five to twenty minutes. (Sihvola 2012)

3.2 Function of each components

In order to provide an improved service and realize additional functions, there are lots of components installed into a computer, to create a kiosk machine. Picture 1 illustrates each component around the kiosk machine, laser printer, credit card reader, document camera, activation button, microphone, web camera, speakers and the place where the customer can picks up the auto key. These components are essential and together they provide quality services for the kiosk user.



Picture 1. The Face2Face Kiosk – technically speaking (Face2Face 2010, Products)

3.3 The structure of the network kiosk system

The working environment of this Face-to-Face kiosk system contains the kiosk device, back office, business partner and the credit card payment company. Figure 2 illustrates how the face-to-face kiosk system works. (Sihvola 2012)

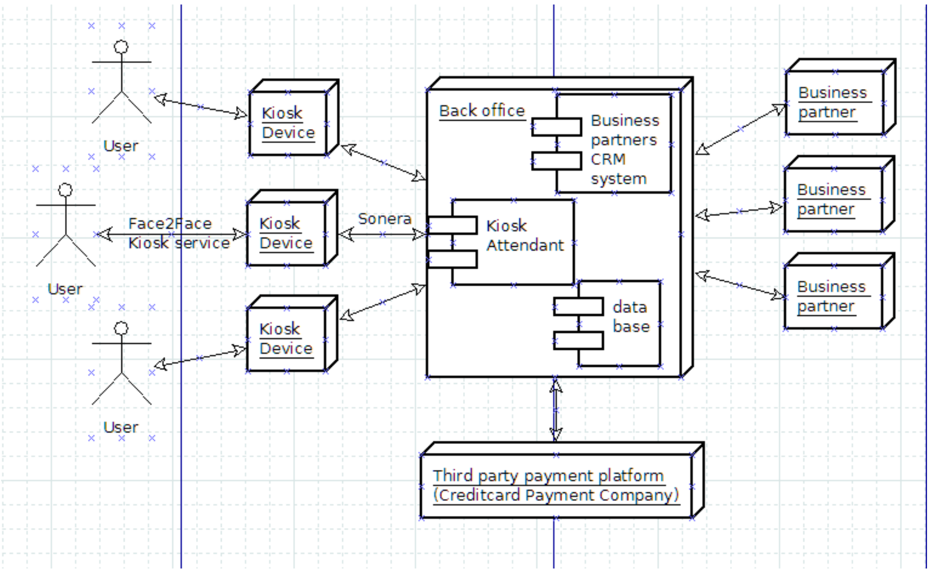


Figure 2. How does face-to-face kiosk work

The internal network of kiosk system is divided into two parts, one is kiosk machine and another is back office. The back office acts as a service supplier which provides the call center service. In the back office, there is a kiosk attendant who will give each of kiosk users to provide the 24 hours a day uninterrupted service, in order to help them better to complete the self-service via audio and video communication. In addition the back-office is connected to the other business partners and the credit card payment company as well. The role of business partner is providing the products for the back-office. The role of third party payment platform is providing the financial management service for the back-office. (Sihvola 2012)

“When users using the kiosk system, the kiosk machine works as a platform which provides the main function requirement, it provides real-time and audio video interaction, printer and scanners service and remotely controlled functions” (Face2Face 2010). This self-service terminal be composed of a PC desktop computer and other peripheral modules, the majority of these modules is used as a serial interface, including touch screen, barcode scanner, the credit card reader, PINPAD, vouchers printer, infrared sensors, a modem…and etc. “These modules convert input/output signals to engineering units and transmit/receive, in ASCII format, to/from any host computer with an RS-232 or RS-485 port” (RTC Group 2008.) All these modules via RS-232 serial communication are the best choice for a balance between security and stability.

In the back office include three small parts, it is respectively is kiosk attendants, data base and Business partners CRM system. There has a unique dedicated internet line in order to connect back office and kiosk machine, at both ends of the line respectively setting up the ADSL modem, providing some protections from their own internal hardware firewall. (Sihvola 2012) Figure 3 illustrate the connection between kiosk device and back-office.

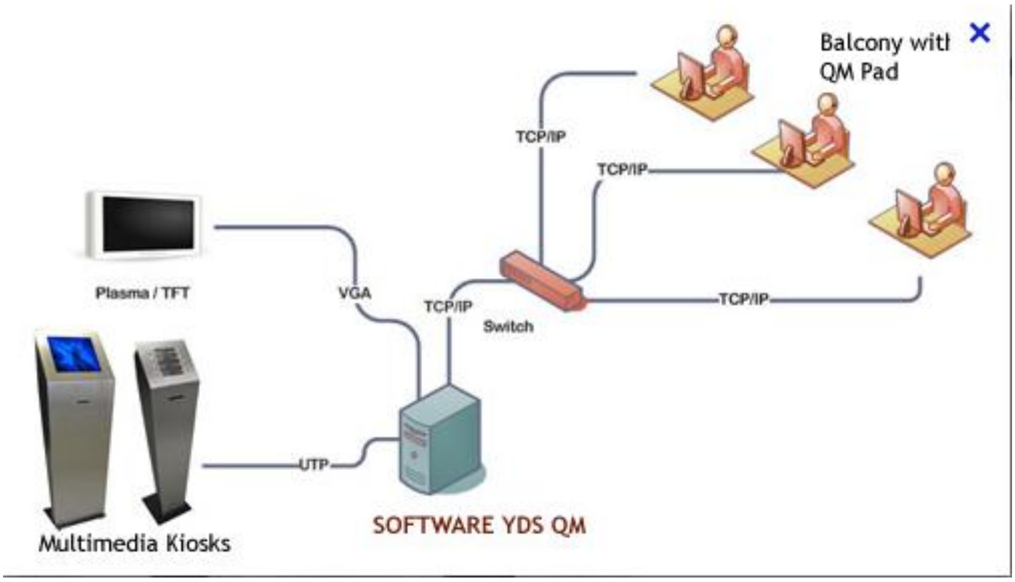


Figure 3. Connection between system and back-office (Crprus Kiosk Company 2010)

They utilize a unique dedicated internet line which provided by Telia Sonera in Finland, it is used to connect between kiosk machine and back office. However, after analysis the safety requirements and budget cost, at the both ends of this line are setting up ADSL and hardware Firewall. Comparison with ADSL, the router can provide more functions, for instance, use a router can use the same name to set up every time, the router is easy to use and is much stronger than ADSL. However, utilize router needs more knowledge to define, and the price of router is ten times of the ADSL, In addition, there are varieties in size as well, the router is double in size than ADSL. Therefore, the final choice is ADSL. It has enough safety in theory. Unless there is evildoer damaging the machine and directly connected to the router port, otherwise, it cannot enter a separate links. Furthermore, both ends of line are equipped with ADSL firewall, even if the evildoers through the one end but also can not be easy to get to the other side.

The data is associated with users' identity information and the credit card information they are collected from the kiosk device, and transmission through this unique dedicated Internet line. This kind of information will be send to the database to process and preserve which is located in the back-office, when it needs to be used, the staff in the back-office can extract the data, and sends it to the appropriate business partner or the credit card payment company.

4 RISK ANALYSIS OF KIOSK SYSTEM

The success or failure of the kiosk largely depends on the wishes of the customer, in the absence of technology to provide enough sure personal and financial information security, some customers will delay using the technology, until they are sure that the information will be in safety control.

The kiosk device must be accepted by an increasing number of people, because it has a large number of advantages. The value of kiosk will be stimulating the interesting of hackers and other criminals, with the continuous improvement of their utilization. For example, in order to get reservation users will input the personal information and information of credit card. Thus, I have to consider the risk of kiosk, “from the event, probability of event occurrence and the effect on the project” (Taylor 2003, 153.)

Analysis the structure of network kiosk system, the security of kiosk is divided into three classifications from the technique. Physical safety to guarantee the safety of the hardware and software without sufferings destroyed, that means no one can destroy or steal anything from the kiosk device through the physical damage. Safety of the operation environment to make sure that the computer in back office is in a safety environment for the normal work. Prevent technical threats and malfunctions happen in the whole network kiosk system. In addition, the information security ensures sensitive information to avoid illegal reading, modifying and leakage, not only in the back office but also in the data transmission process. In order to defense the communication and software threats.

The author according to reflect from the functions of each parts and analysis their risks. This system contains kiosk machine and back office. The sensitive information includes the data of personal ID and information of credit card, and both of them are input from kiosk machine. It will transfer by unique dedicated internet line and stored into database which is located in the back office. Sometimes, the back office provides a third party payment platform in this B2C business models. Thus, the major risks of this network kiosk system are in the back office.

4.1 Risk analysis from physical safety point of view

“Typically, users can not complete the following operations, i.e. install programs, tamper with kiosk software, access the underlying operating file system, or view data entered by other users” (Smith 2008.) In some functions related to the security system in the kiosk machine, they involve collecting information and transmitting data to the database. In addition, in the car rental process, the kiosk device also needs to conserve the car key. Therefore, in this process the kiosk device can only suffers from physical damage. For instance such damage may take place when a suspect uses the tool for tapping, shakes the machine or cuts off the power of the machine in order to obtain benefits from the machine. Moreover, the suspect may destroy the cabinet in the kiosk device to steal the auto key.

4.2 Risk analysis from the technical threats or malfunctions point of view

By investigating the entire remotely served customer service concept, the kiosk machine is merely a tool to provide the service. However, the real service provider and sensitive data are kept in the back office. In this thesis, the hardware or system malfunction in the back office is the most significant part needed to be protected. For example, people can use the kiosk to rent a car. When all of the correct operations are finished the cabinet is still closed. Another risk is created if a hacker attacks and controls the back office and opens the cabinet without any operations. There are two reasons for this situation. One reason may be that the back office is captured by the hacker, and another reason is that the network of the system is attacked by malicious resource-intensive, no longer controlled by the staff of back office.

The malfunctions are not only happened in the back office, but also happened in the kiosk device. The malfunctions happened in the printer and credit card reader, or even occurring power failure in the middle of transactions. Fortunately, each kiosk device has UPS which will starts automatically after power failure and keep available for 5 to 20 minutes, and users do not worry about power failure during the transactions. Therefore, the author also needs to think about what will be the solutions if this kind of incidents happened. Table 1 illustrates the probability of each risk of network kiosk system.

Table 1. Analysis the risk of network kiosk system

Risks	Very Low 0-5%	Low 6-15%	Medium 16-40%	High 41-80%	Very High 81-100%
Natural disaster	1%				
Software error		7%			
Human error		11%			
Virus	2%				
Hardware or system malfunction				79%	

The back office security should consider the network security at first. The network system faces the several main performance security threats. Such threats include the following: identity thefts, unauthorized access, data breaches, denial of service, viruses and malware attack, pretentions to be legitimate users. The attacks from hackers invade will make the attacker to obtain the important information from other users illegally. Generally, hackers always used computer viruses to make the network cannot work normally, or even cause the whole network to paralyze. For example the denial of service attack, it is making the user receive a large number of useless E-mails in a very short period of time. Risks need to be analyzed in order to secure the business from the hackers' point of view. For example, the external attacker can find and collect the credit card information from a database server. Or the remotely unprotected computer is infected with viruses defective due to operating system vulnerabilities. (Reuvid 2006, 86)

“The vulnerabilities can be sorted into following five: environment and infrastructure vulnerabilities, hardware vulnerabilities, software vulnerabilities, communication vulnerabilities, and personnel vulnerabilities” (Furnell & Katsikas & Lopez 2008, 8.) As the user is in-depth use, the system will continue to be exposed to the existing vulnerabilities. System vendors will release patches to repair the previously discovered vulnerabilities, but also introduced some new bugs and errors. Therefore, the problem of vulnerabilities will exist for a long time which also has growing into a trend. In addition, the threats of network security will increase with the growing number of vulnerabilities as well. Figure 4 illustrate the growth rate of vulnerability in 2000 to 2007 (Furnell & Katsikas & Lopez 2008, 9.)

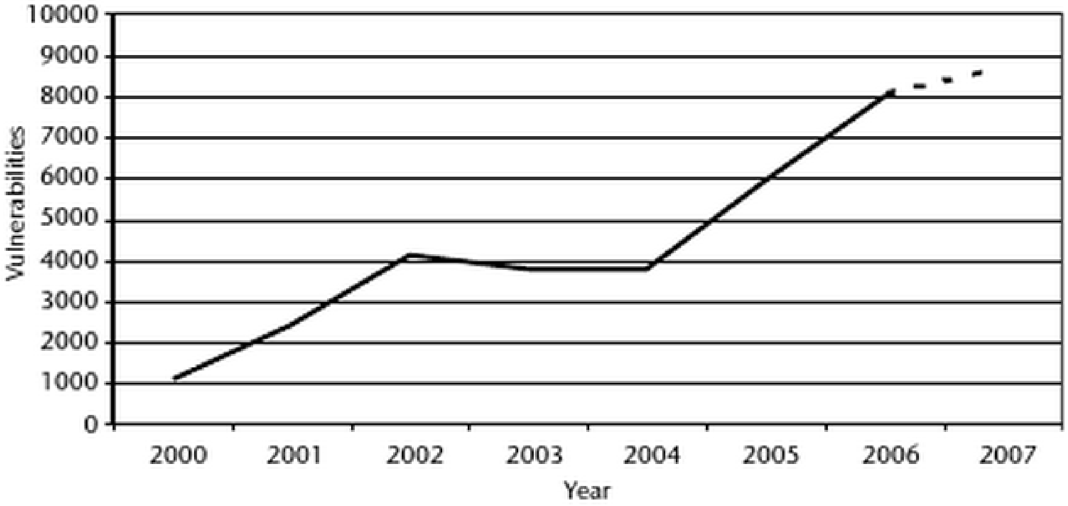


Figure 4. CERT/CC vulnerability statistics from 2000-2007 (Furnell & Katsikas & Lopez 2008, 9)

If the hacker attacks the back office through the Internet to make an incursion, once the hacker attacks success, hacker can peep, steal or distort the sensitive information in the back office. Even more, direct control the back-office and replace the function of back-office to control the kiosk device to gain the illegal benefits.

Another case is the hacker continuous to occupy the flow of the kiosk system, until the system was paralyzed due to excess load. The denial of service attack is one example of this. “The purpose of denial of service attack is to prevent legitimate users having access to the normal network resources.” Therefore, all of the attack which can lead to legitimate users can not be normal network services considering a denial of service attack. Furthermore, this is an example of the information security risk from technical threats (Milutinovic & Patricelli 2002, 271-273.)

“One type of DoS attack exploits a flaw that causes the service or server to crash, making it unable to service users’ requests. Another form of DoS involves general service requests to a Web server at such a high rate that the server is unable to respond to legitimate users’ requests.” (Hollar & Murphy 2005, 51), and “Most of these attacks use technical means rather than physical attacks”. The basic process of DoS attacks are as follows. First, the attacker sends requests to the server with many a false address. The server cannot wait for the return news because the address is forged and the resources allocated to this request have not been released. When the connection will be cut off because of timeout, the attacker will send a new batch of requests with pseudo-address once again, until the resources of server will eventually be exhausted.

“With the development of computer and network technology and with the rapid growth of computer processing power and memory, the target computer has enough resources to cope with common DoS attacks. This will undoubtedly increase the difficulty degree of DoS attacks and reduce the effect of DoS attacks.” However, unfortunately, this development has made the DDoS attacks came into being. (Knowwordlib 2011)

The DDoS attacks are getting through controlled a number of machines to attack one machine. The DDoS attacks consist of the following four parts. There are attackers, hosts, the attack port of proxy servers and victims. Figure 5 illustrates the schematic nature of the DDoS attacks.

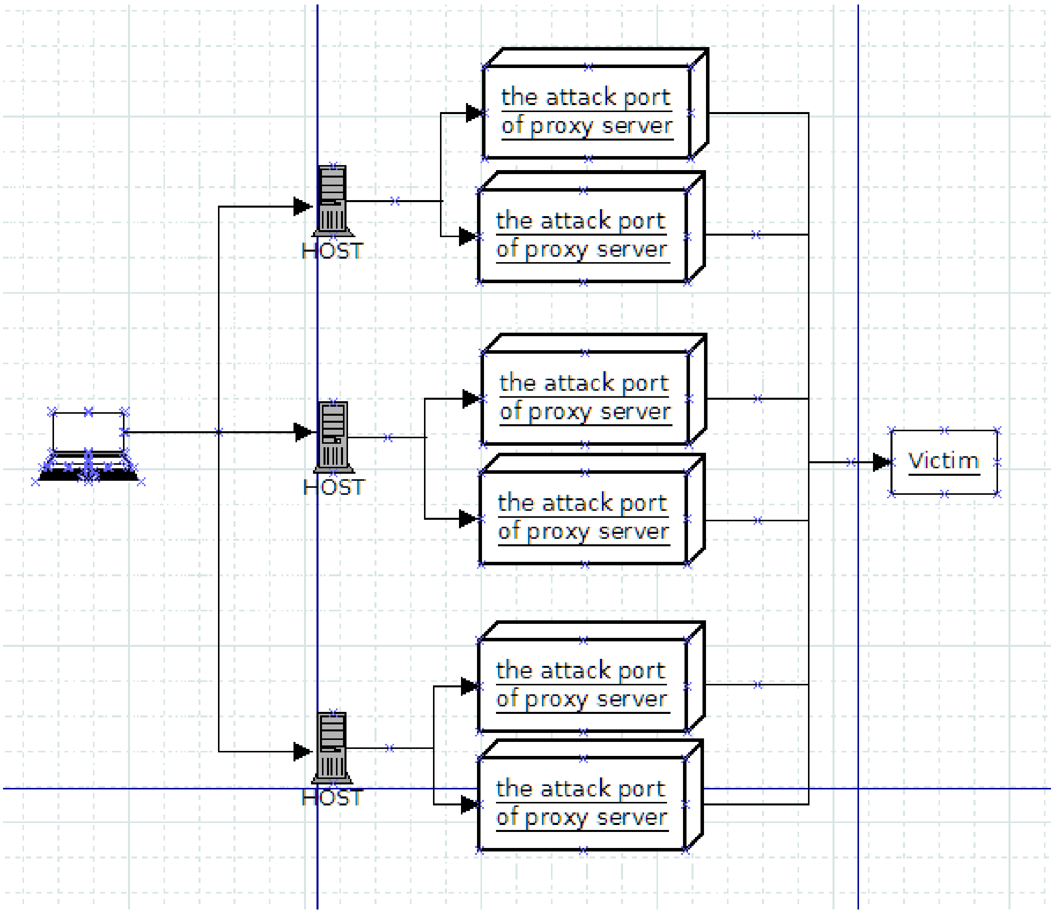

HOST
HOST
HOST
the attack port of proxy server
the attack port of proxy server
the attack port of proxy server
the attack port of proxy server
the attack port of proxy server
the attack port of proxy server
Victim

Figure 5. The schematic nature of the DDoS attacks

The DDoS attacks include the following three steps. First, the attacker needs to collect the target information, which contains the address of the target host, configuration, performance and bandwidth. In the step to follow, the hacker needs to occupy and control the host server being attacked, in order to distribute to host servers and proxy servers. Finally, after receiving the commands from the attacker, all of them get an order to launch a unified attack. It will make the victim receive a large number of useless information in a short period of time, a lot of system resources are occupied at the same time. The DDoS attacks cause that the system cannot work normally, and even a crash is possible (Kuinam & Seong 2011).

Besides these direct DDoS attacks, there still is another indirect DDoS attack, which has a larger potential and is more subtle than direct attacks. The difference between the direct attacks and indirect attacks is the SYN connection request packet sent to the larger number of servers to be the victim's address, after the attacker forges the source address. (Kimberly 2007) Then, the group of servers will issue a large number of SYN and ACK or RST packets to the victim (Belapurkar & Chakrabarti & Ponnapalli 2009, 72-82.) Eventually, crash or system halted because the system needs to responds to a large number of the server's response packet. Figure 6 illustrates the schematic of this indirectly DDoS attacks (Tselentis & Galis & Gavras 2010, 127-128.)

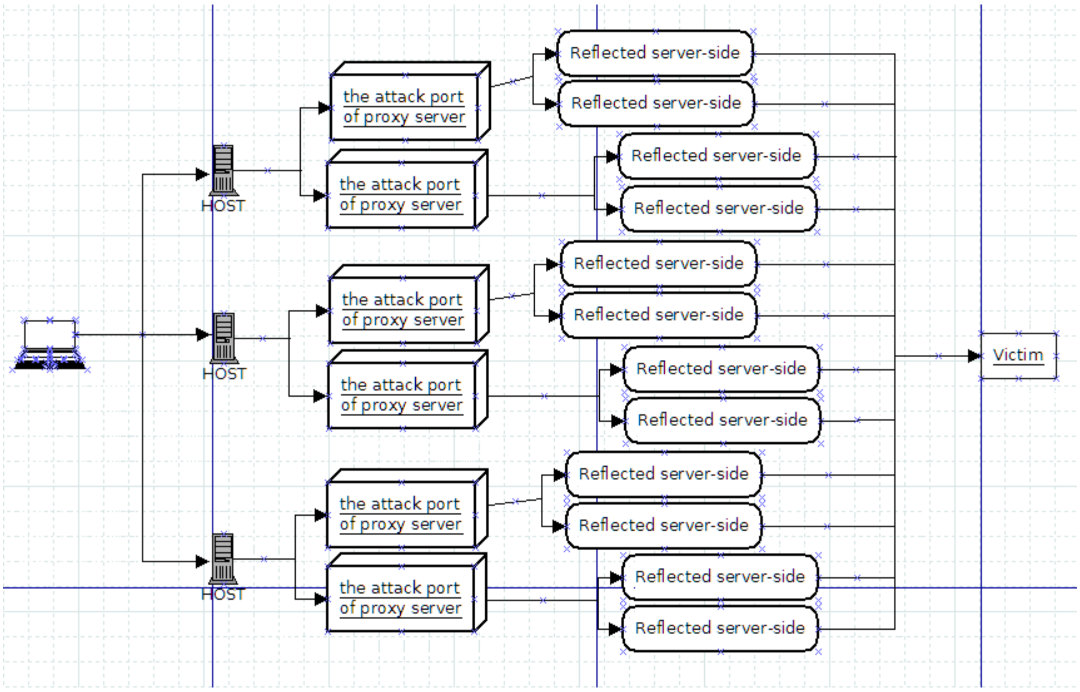

HOST
HOST
HOST
the attack port of proxy server
the attack port of proxy server
the attack port of proxy server
the attack port of proxy server
the attack port of proxy server
the attack port of proxy server
Reflected server-side
Victim

Figure 6. The schematic of indirectly DDoS attacks

4.3 Risk analysis from communication and software threats points of view

There are two kinds of data transmission processes. One is between the kiosk device and the back office, and it is relatively safe because it uses a unique line to transmission. Another process is between the back office and their business partners, and it has more threats because each company has various levels of security. The only risk in credit card charging is if somebody will get access to the credit card number, during the swipe phase or when transferring the card reading from kiosk to the credit card payment company through the business partner CRM system. The administrator needs to control the security of the swipe process and transferring the reading to the CRM system. (Sihvola 2012)

“The actual threat from hackers and viruses is much smaller than most people would anticipate” (Tworek & Chiesa & Dahm & Hinkle & Mason & Milza & Smith 2004, 49), “In fact, in the organization security the major of security incidents are caused by internal factors. However, the human factor is dominant in all the internal factors”. Figure 7 illustrates the insider attacks and other threats.

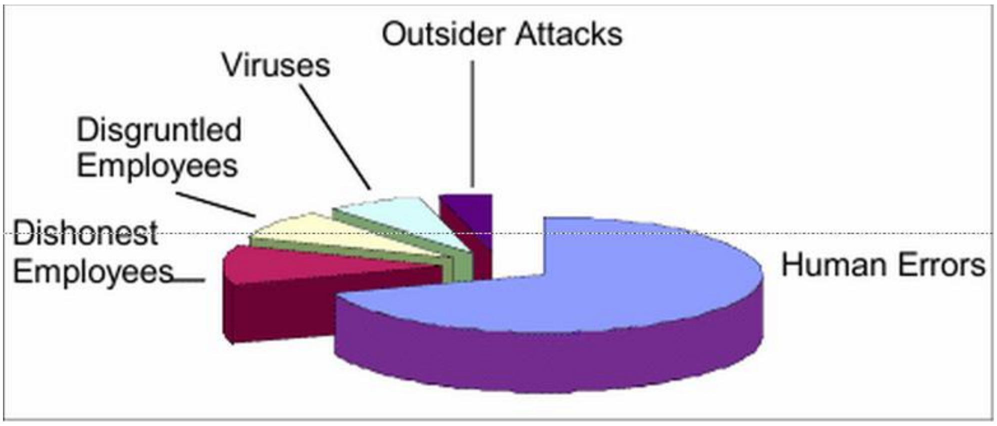


Figure 7. Insider attacks and other threats (Tworek & Chiesa & Dahm & Hinkle & Mason & Milza & Smith 2004, 49)

In addition, because weak awareness of our own information security, or do not have fully communication before cooperation. It will cause the information threats from a variety of different starting points. Such as in table 2, it is not a good choice no matter too much trust or excessive demands between company and security vendor. The following table lists some of the considerations, the company and the security providers are focus on a slightly difference in each of regions.

Table 2. Vary consideration between the company and the security providers (Blyth 2008, 7)

Expectations	Impacts	Risk Focus
Company payment tied to schedule	More inclined to take risks to ensure timely project completion	Low
Company payment tied to performance	More inclined to allocate monies to mitigate risks during contract	High
Company has low risk threshold	Maybe with draw from project if risks increase or injuries occur, or invest in risk mitigation	High
Company accepts high risk threshold	Higher probability analysis that risks are accepted; possible cavalier attitude and lower investment in risk mitigation	Low
Company defers security responsibilities to vendors	Company may force definitive provider agreements to achieve project needs and may demand unrealistic or high-risk services from security vendors	Low
Company dependent on security provider/vendor for decision making	Company reliance may result in greater acceptance of advice and guidance, limiting the ability to conduct quality assurance of security vendors	High
Security vendor values its own reputation	Security vendor may refuse work, or take a strong	Varies

	position on accepting risk in order to protect its reputation or liability exposure	
Security vendor’s business development goals important	Security vendor may accept higher-than-normal risks in order to grow business quickly	Low
Security vendor has low liability tolerances	Greater focus on liability risks, especially injuries and deaths, thus driving more candid and realistic recommendations and approaches	High
Security vendor’s experience in service	Experience varies the balance of company/risk/business needs	Varies
Risks posed direct to project	Threats posed directly to a project result in greater focus on risk through specific project-targeting threats.	High
General risks high for region	General risks may result in more balance between project needs and risk levels	Medium
Project faces low risks	Low risk levels may result on a greater focus on the business needs	Low
Only provider faces risks	Providers who face all risks focus on their own business needs; companies may accept higher risk levels as they will not be affected	Varies

Moreover, software threats are another part of affecting data security. The kiosk system is equipped with some basic protection techniques, such as the firewall. Firewall is a defense system which is isolating the internal network and external network, controlling the communication between two networks. It follows a kind of communication to allow or deny between the network securities mechanisms, only allowing the authorized traffic. Thus, the main work of the firewall is to control the data and access, and record network activity. According to different requirements, the functionality of the firewall is quite different. “At present, some main technical specifications of firewall are the packet filtering, application gateways, proxy server, etc.” (QuinStreet 2012, Firewall) However, it still has some shortages of firewall technology in network security or firewall prevention. “Such as the firewall cannot prevent the internal attack and cannot replace the anti-virus software. In addition, the firewall cannot easily prevent Trojan rebound port attacks” (Security Awareness 2010.)

In addition, for a complete and secure network security system, it not only needs an active protection system to protect security before being attacked and takes an effective defense measures during the attacks, but also a capacity of data repair. If the risk cannot be avoided, the company needs to ponder over how to reduce the losses. No matter what the data losses or modifications, the company needs to consider the data backup and recovery.

5 RESULTS

The author analysis and summarizes the information security risks for the kiosk system. They are mainly from the physical destruction of kiosk machine, such as malicious damage of human destruction. From the technical threats or malfunctions are the system attacked by virus and DoS attacks. As well as from the communication and software threats are the data transferring threats and human factors. Therefore, in order to give some safety recommendations of the ETA Company before they create their platform, the author plan to prepare a few programs as follows.

5.1 Physical protection

“The physical risks such as crime, insurgency, terrorism, civil unrest and natural disasters are the unpredictable event and have significant impacts on companies and individuals. Risk mitigation, planning for contingency, and planning for crisis can be used to offset the spectrum of the risks” (Blyth 2008, 109.) Under ordinary circumstances, the case company’s kiosk machine was set up at the public place where manned police station. Thus, I suggest it can combine an audible and visual alarm with the kiosk machine in order to protect the kiosk machine from physical threats. When vandals attempt to undermine a kiosk machine, the kiosk will automatically trigger an alarm of audible and visual alarm device. In order to attract the nearby police attention, the camera which is set up at the machine will record the criminal process. Figure 8 illustrates the effect after implementation of the author’s suggestion. When the owner of the machine cuts off the hidden power switch, it is the unique method that can stop the alert. This alarming apparatus has high stability whose lamp has a long life and provides standby power. It can be used to monitor whack, vibration, tilt and other physical damage, in addition, thanks to the use of sealed shock vibration sensors, and it is without interference by the wind.

Figure 8. Kiosk with audible and visual alarm

The most significant part of audible and visual alarm is a vibration sensor detector. “Provided for adjusting the analog channel gain control to optimize operation of the monitor for varying machining conditions based on machine tool control information which is communicated to the monitor” (Thomas & Lee & Bedard & Hayashi & Harris 1988.) when the digital vibration detector combines with a microprocessor control. For the strong vibration or accumulating many times vibration will be considered a valid signal, which can generate alerts and it will be stored in the pulse count memory. However, the weak signal of vibration will be shielded automatically. In addition, it can be adjust manually the degree of sensitivity, in order to achieve flexible operating.

The digital vibration sensor detector is used to prevent various types and different sizes of safe equipments, such as ATM and the kiosk. “These vibrations excite the acoustic sensor processor which passes the frequency through a filter, compares the frequency for a match and signals an alarm if appropriate” (Irv 1997, 32.) It uses the principle of acoustic vibration sensing and with the CPU processing technology, combining a vibration sensors and vibration analyzer into one. It will effectively prevent the equipment smashing, drilling, prying and other disruptive behavior occurrence. Normally closed output is generic with all brands of wired alarm host, DVR and matrix controller support. In addition, the characteristics of this detector are as follows, it has a small size, easy installation and stable performance, and it widely used to prevent the occurrence of any percussion and disruptive behavior.

5.2 Technical and malfunctions protection

The Influence factors of network security are as follows: the safety of the node, data security which contains data saves and data transmission process and the safety of the documents, etc. The network security of network kiosk system focuses on the anti-virus and anti-attack in the back office. Therefore, aimed at the characteristics of the virus and cyber attacks, in order to puts forward the security protection measures for network kiosk system.

The network information security is a complex system which involves a lot of aspects. A complete network security system should include at least three kinds of protection measures. The first measure is legal policy, rules and regulations, safety education and external software environment. The second measure is in technology, such as information encryption of storage and transmission, identity authentication, firewall technology, network anti-virus, etc. The third measure is a management measure of technology and social measures. The main measures are providing a real-time change of the security strategy and real-time monitoring enterprise safety status (AllBusiness 2004).

“Intrusion detection systems, firewalls, anti-virus software, virtual private networks, encryption and biometrics are security technologies in use today” (Hentea 2012.) Therefore, the security structure of network kiosk system should consider configuring defense system. It is contains firewall technology, virtual private network technology, network encryption technology, identity authentication technology, multi-level anti-virus system.

I suggest the ETA Company needs to build a virtual private network (hereinafter VPN) between the back office and other business partners, in order to reduce the percentages of being attacked by hackers. “The VPN is on the public network via a dedicated channel on the Internet to create a secure private connection. This network is created to connect remote users, back office, business partners and the company’s corporate network through a secure data channel, to achieve the purpose of the extended enterprise network” (Lucas & Singh & Liu 2006.) In addition, the VPN provides the following four functions: data encryption, message authentication, identity authentication and access control.

The first step of building the VPN is to establish a VPN server. The second step is to assign the permissions of remotely accessing users, and after that generate an Internet connection in the VPN client. The next step entails establishing a VPN dial-up connection for the VPN clients. The final step is to establish a connection among VPN clients, the VPN server and Internet connection (Equinux AG and equinux USA 2010).

There are several available options in order to minimize the DDoS attacks, “including keeping the security profile current: profiling traffic patterns; splitting DNS infrastructure; exploiting load balancing; tightening firewall configurations; safeguarding perimeter devices and utilizing traffic shaping; carry out an IDS, vulnerability scanner, or proxy server; taking snapshots and conducting integrity checks of existing configurations; allocating sacrificial hosts; improving network and host management; maintaining a response procedure; and arranging more secure technologies” (Russell & Huston 2000, 115.)

Thus, people are faced with the increasingly serious DDoS attack, the administrator needs to reduce the possibility of attack. Firstly, the administrator should ensure that all servers use the latest system and patched software of vulnerabilities. In addition, the administrator needs to establish and improve the backup mechanism for some important information, such as system configuration information, especially when setting some privileged account, such as the administrator account. Secondly, it is necessary to delete redundant network services and establish the boundary of security. Moreover, it is necessary to ensure that the package of output is properly restricted. Thirdly, it is necessary to exploit network security devices to reinforce the security of the network, for example, hardware firewall. Further, it is necessary to filter out all possible forged packets. Moreover, carefully check privileged ports and non-privileged ports.

In order to avoid when the printer or credit card reader does not work to influencing normally work of the kiosk system, I put forward the following two points of plans. The purpose of this plan is to propose a remedy when the printer or credit card reader does not working. If the malfunctions happened in the printer, the system will ask the user to enter their phone numbers, then, the contract will send to the user's mobile phone by SMS. If the malfunctions happened in the credit card reader, the system will ask the user to enter their credit card number, then, the credit card information will recorded into database. Figure 9 and Figure 10 illustrates the solution about the malfunction happened in the printer and the solution about the malfunction happened in the credit card reader respectively.

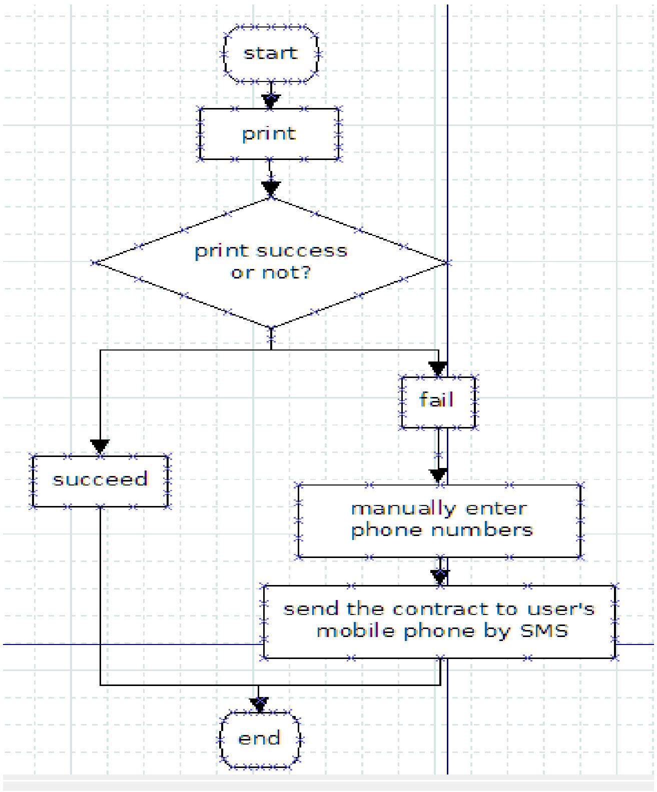


Figure 9. Solution about the malfunctions happened in the printer

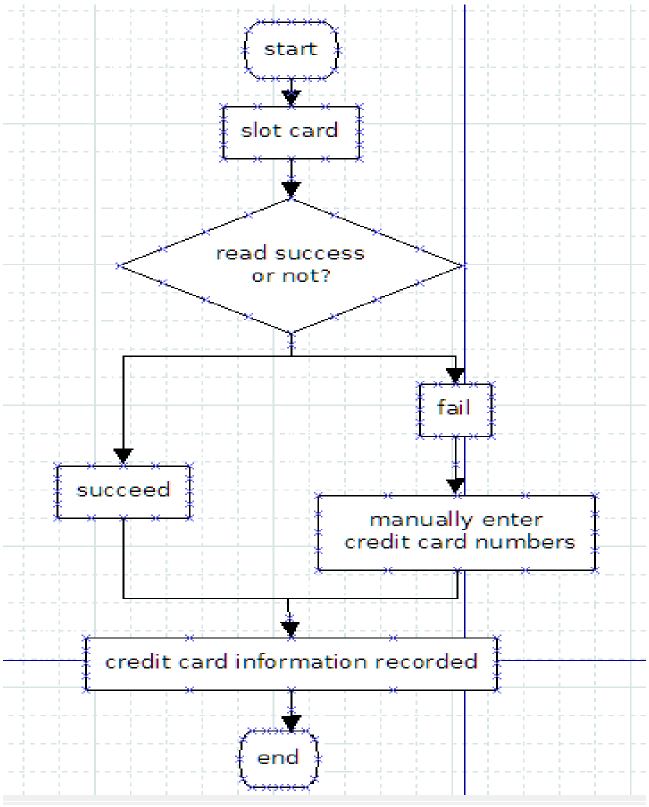

start
slot card
read success or not?
fail
succeed
manually enter credit card numbers
credit card information recorded
end

Figure 10. Solution about malfunction happened in the credit card reader

5.3 Data protection

Data security contains two parts, one is security of data another is data safety protection. The basic measure for the security of data is uses modern cryptographic algorithm in order to protect data actively, for instance, data confidentiality, data integrity and mutual authentication.

5.3.1 Smart card

In China, when one is in a bank for a large transaction, there will be an interesting situation. The handling of the entire process is completed by two people, one is the bank teller that the customer faces, and another is the duty manager in this bank. Each duty manager has a smart card which is used to confirm the transaction. This is the only way to accomplish large transactions in banks.

These give me an idea that each of duty managers in this network kiosk system should have a smart card, which is used to confirm the commands and the data encryption. Before data transmission from database, the duty manager must insert a smart card to encryption of the data. Then, when the legitimate of the recipients receiving the data, it also needs to used the smart card for decryption of data. Besides, the smart card can automatically identify whether the data has been modified.

With a relatively high calculation request on the card, “there is a secret key involved in many of these cryptographic protocols which is stored on the card, in order that it can be used to perform the encryption operations directly.” (Furnell & Katsikas & Lopez 2008, 193-194,) “In currently highest security level, smart card used for banking applications and digital signatures. It includes the coprocessors for encryption application, sensors for active tampering detection, and the known solution against attacks.”

For the data safety protection, the basic approach is the administrators use modern information storage to active protection, for instance, RAID (Redundant Array of Independent Disks), data backup and A method on quick disaster recovery in disaster-tolerant system is presented and realized. In order to achieve the data repair after being attacked. The implementation of hardware array is to use a dedicated disk card. The hardware array can provide online expansion, dynamic modify the level of array, automatic data recovery, drive roaming, ultra-high speed buffer and other functions. It can provide performance, data protection, reliability, availability and manageability of solutions. Not only the performance is much higher than the conventional non-array drives, but also more secures and stable.

5.3.2 RAID

“RAID configuration to ensure continuous operation in the event of disk failure” (Somasundaram & Shrivastava 2010, 239.) The principle of RAID is to use a way of array to a disk pack, with the design of data scattered arrangement and enhance the security of data. Use this technology in order to cutting the data to the number of sections, leave with them in each hard disk respectively. Furthermore, RAID can use the concept of parity check to read the data in the array when either a hard drive failure. The administrator needs to put the data into new hard drive after recalculation whiles the data reconstruction.

“The reading and writing of the data are done in a simultaneous process” (RAID Data Recovery 2006.) The advantages of the RAID are to improve the speed of data transmission and through the data validation to provide fault-tolerant function. RAID on multiple disks to store and read the data at the same time, in order to implement the data throughput of the storage system which has certainly improved. In RAID, one can make a lot of disk drives transmission of data simultaneously.

Ordinary disk drives cannot provide the function of fault-tolerant, but the RAID could, “ A category of disk drives that employ two or more drives in combination for fault tolerance and performance” (QuinStreet 2012, RAID.) it provides a higher safety. In many ways RAID modes have a complete mutual check and recovery measures, even the directly with mirror backup with each other. Thus greatly improving the fault-tolerance of RAID systems and improving the stability of the system redundancy.

5.3.3 Data backup

As for a complete network security system, it is not enough for only providing prevention and detection measures, but also it should have the capabilities of disaster tolerance and system recovery. This requires that even in the event of a system disaster, it still can restore systems and data quickly. In order to provide fully protect the security of the network information system.

Data backup is preserve date by create a copy of the data. To prevent the original data are being deleted, covered with, or unable to access due to fault. However, it can use the copy to restore lost or corrupted data. Date recovery is to let the marred data, inaccessible data due to hardware defects, and data lost due to misuse. It is make the lost data to restore to be normal data. For computer applications system, data can be divided into system data and user data. However, user data is priceless, such as personal ID information and credit card information. Recovering it is particularly important. From the test result of a variety of data recovery software effect, coordinate with Easy Recovery and Final Data can obtained a better recovery effect.

Easy Recovery is a powerful hard disk data recovery tools launched by a world-renowned data recovery company, "support for remote restore function, have a variety of scanning filter methods, high success rate for the data recovery and is easy to use" (Kroll Ontrack 2012.) However the Final Data recovery of deleted files by scanning the disk, it does not rely on the information records in the directory entry and file allocation table. Thus, "it can not only recover deleted files, but also recoveries the data in the case a whole file allocation table is destroyed in the directory entry. Even recovery the data in the disk boot sector is damaged or loses the entire partition information" (AOS Technologies 2012, Overview.)

Compare with earlier data recovery products, Final Data has the following six characteristics. There is easy operation that means both interface style and operation methods are similar with Windows resource manager. For the recovery speed, it can restore more files or restore directory remains the same structure. Final Data support various operating systems and without pre-installed, after the accident can be operating in Final Data from the CD. In addition, it provides data security to computer across the network and it is full support for double-byte file recovery, such as FAT, FAT32 and NTFS file. (AOS Technologies 2012, FinalData Standard)

5.3.4 A disaster-tolerant system

Construct emergencies help ETA Company tolerate a disaster or chief interrupt service with HP Disaster Tolerant and constantly computing solutions. "HP disaster tolerant and constantly computing solution helps ETA Company to protect their IT operations and data among the geographical distributed sites data replication, failover and storage capabilities" (Hewlett-Packard 2011), "HP disaster recovery solution integrated with the HP Storage works array-based data replication and remote mirroring software, and operating system-specific cluster solution. With these seamless integrations, the HP disaster recovery to solve the program providing a key to opening the recovery from a catastrophic event, in addition, enduring commercial downtime crucial difference.” These solutions could provide mitigate risk, improve IT availability and reduce costs of downtime of ETA Company, for example, it can minimize direct financial impact, prevent impact from reputation, improving the productivity, customer experience and time to recovery, besides, it reduce the resources required.

6 DISCUSSION AND CONCLUSIONS

In this chapter, it shows the result of the author’s thesis, limitation and challenges of the research project, also the further development and conclusions of the author’s thesis work.

6.1 Result of my thesis

Firstly, this thesis analyzes the major harms of the ETA Company network kiosk system faces. It is divided into three parts, one is threats of kiosk devices, one is threats of back office, and the third is threats during the data transmission. People are afraid of the vandalism, causing some valuable items to be stolen from the inside of the machine. The author suggests combining an audible and visual alarm into the kiosk device, the alarm will alert when the kiosk device is being attacked. In addition, coordinate with the camera which one is set up in the kiosk device, it will record the criminal process when the kiosk device is being attacked. This is an effective method in order to reduce the incidence of such events.

Moreover, the malfunctions also happened in the kiosk device, such as printer or credit card reader. The author put forward the solution to solve these kinds of incidents. The back office is seen as a service provider which needs to offer the real-time service, with a connection between the kiosk device and their business partners. There is need to configure a series of active defense systems, such as anti-virus and the technology of VPN. The system failures are not allowed as a company engaged in the remote service platform. The back office will suffer from some hacker’s attacks. The DDoS attacks can be a main attack way, which makes the system to paralyze. The author put forward some methods trying to avoid or reduce suffering from this kind of attacks.

The process of data transfer is the most dangerous state for the data security. Therefore, the author suggests using a smart card for encryption or decryption before the data transfers. In addition, the author also makes suggestions for the data recovery part. RAID simultaneously provides a lot of drives of data transmission, by means of coordinate with Easy Recovery and Final Data getting a better recovery effect. Moreover, HP disaster recovery solution provides a tool for mitigating risk, improving IT availability, and reducing the cost of downtime of the ETA case company.

6.2 Self-evaluation of my work

Gradually, under the guidance of supervisor, I began to have a direction of my thesis. I learned how to collect information through a lot of reading, accumulated the knowledge of risk analysis and management. In addition, I increased the study experience for my future life.

Firstly, I collected the relevant data of the network kiosk system. Secondly, I conducted a risk management of the information security in the network kiosk system. The threats found are the information risk from physical threats point of view, the information risk from technical threats or malfunctions point of view and the information risk from the communication and software threats point of view. I collected data of information security from scientific resources and literature, such as libraries, formal PDF documents and personal interview with the CEO of ETA Company. Then, drew a conclusion and provided a combination of suggestions of experts' views.

In order to establish effective security procedures, I needed to understand the current threat levels and organizational vulnerabilities. Using the above measures, I could provide suggestions for resolving the basic risks of the network kiosk system, in order to build a safe and efficient network. The whole research was a process for looking for six feasible methods to improve the security system for the ETA Company. The first method is to put an audible and visual alarm into the kiosk device to improve the physical protection. The second method is to establish a Virtual Private Network to connect remotely users and business partners, in order to reduce the percentages of being attacked. The third method is properly set up a computer in order to avoid and reduce the DDoS attacks. The fourth method is put forward the solution about malfunctions happened in the printer or credit card reader. The fifth method is suggested using a smart card to keep the security of sensitive data. And the final method is put forward a solution to achieving the data repair after it is attacked by RAID, data backup or a disaster-tolerant system.

6.3 Suggestions for further research

“Our technological powers increase, but the side effects and potential hazards also escalate” (Toffler, 2011). A network kiosk system without guarantees of the network security, it is just like the car without brake running on the highway. With the rapid development of the Internet, it has produced a far-reaching impact on the employees and customers of the network kiosk system. Because the networks have become ubiquitous in our lives, as enjoy the high-tech to bring us convenience, people need a clear understanding of network security issues which are becoming increasingly serious and increasingly become a great obstacle to network applications at the same time. The network security of network kiosk system has come to a condition that it must be unified managed and completely resolved. Only by solving the issue of network security, the network applications of the network kiosk system can be healthy and high-speed development.

In sum, the question of how much security is enough is an important question to answer. Information security is a never-ending work. (Soo Hoo 2000, iv) I cannot be sure if there is a new kind of attack method or risks to appear when I finish this thesis. The ETA Company plan to do their official business in August, I wish my thesis will to reduce the time and cost on the enterprise security research. Hopefully this treatise can provide a guideline to improve the security of kiosk system for all of this company, which used remotely served customer service concept to do their business.

REFERENCES

Printed

Belapurkar, Abhijit & Chakrabarti, Anirban & Ponnapalli, Harigopal K. B 2009. Distributed Systems Security: Issues, Processes and Solutions. Wiley. Hoboken, NJ, USA.

Blyth, Michael 2008. Risk and Security Management: Protecting People and Sites Worldwide. Wiley. Hoboken, NJ, USA.

Furnell, Steven & Katsikas, Sokratis & Lopez, Javier 2008. Securing Information and Communications Systems: Principles, Technologies, and Applications. Artech House. Norwood, MA, USA.

Hollar, Rickland & Murphy, Richard. 2005. Enterprise Web Services Security.

Irv, Smietan 1997. Defense Advanced Research Projects Agency (DARPA) Joint Program Steering Group, Arlington, Virginia.

Johnson, Gail 2002. Research Methods for Public Administrators. Greenwood Press. Westport, CT, USA.

Kasanen, Eero & Lukka, Kari & Siitonen, Arto 1993. The Constructive Approach in Management Accounting Research. Journal of Management Accounting Research, 5 (1).

Knowwordlib. Com 2011. DDoS: The concept of DDoS attacks.

Krishnaswami, O. R. & Satyaprasad, B. G. 2010. Business Research Methods. Global Media. Mumbai, IND.

Lucas, Mark & Singh, Abhishek & Liu, Dale 2006. Firewall Policies and VPN Configurations. Syngress Publishing. Rockland, MA, USA.

Milutinovic, Veljko & Patricelli, F 2002. E-Business and E-Challenges. IOS Press. Amsterdam, NLD.

Reuvid, Jonathan 2006. Secure Online Business Handbook: A Practical Guide to Risk Management and Business Continuity. 4th Edition. Kogan Page Ltd. London, GBR.

Rugg, Gordon 2008. Using Statistics: A Gentle Introduction. Open University Press. Buckingham, GBR.

Russell, Ryan & Huston, L Brent 2000. Hack Proofing Your E-Commerce Site: The Only Way to Stop a Hacker is to Think Like One. Syngress Publishing. Rockland, MA, USA.

SANS, Institute 2003. The Internal Threat to Security Or Users Can Really Mess Things Up.

Somasundaram, G & Shrivastava, Alok 2004. Information Storage and Management: Storing, Managing, and Protecting Digital Information. EMC Publishing Company. Wiley. Hoboken, NJ, USA.

Soo Hoo, Kevin J 2000. How Much Is Enough? A Risk-Management Approach to Computer Security.

Strebe, Matthew 2004. Network Security Foundations. Sybex. Alameda, CA, USA.

Taylor, James 2003. Managing Information Technology Projects: Applying Project Management Strategies to Software, Hardware, and Integration Initiatives. AMACOM Books. New York, NY, USA.

Tselentis, G & Galis, A & Gavras, A 2010. Towards the Future Internet: Emerging Trends from European Research. IOS Press. Amsterdam, NLD.

Sihvola, Vesa 2012. Interview of Mr Sihvola Vesa, The CEO of Bothnialnvent AB. Conduced on March 12, 2012.

Tworek, William & Chiesa, George & Dahm, Frederic & Hinkle, David & Mason, Amanda & Milza, Matthew & Smith, Amy 2004. Lotus Security Handbook. IBM Redbooks. IBM. Durham, NC, USA.

Not printed

AllBusiness.com, Inc 2012. How Do You Protect You Network Against Hackers. Downloaded April 18, 2012. <http://www.allbusiness.com/technology/computer-networking-network-security-hacking/1529-1.html>

AOS Technologies, Inc 2012. FinalData Product Information. Overview. Downloaded April 11, 2012. < http://finaldata2.com/products/products_overview.php>

AOS Technologies, Inc 2012. FinalData Standard 2.0: Complete, Do-It-Yourself Recovery. Downloaded April 11, 2012. < http://finaldata2.com/products/products_fd_stand.php>

Avis Rent A Car System, LLC 2012. Avis Location Information. Additional Location Information, PREFERED SERVICE. Downloaded March 12, 2012. <http://locations.avis.com/ca/sacramento/smf.html>

Cyprus Kiosk Company 2010. YDS Software Services & Queue Management. Downloaded March 22, 2012. <http://www.cypruskioskcompany.com/index_2010_v2.php?page=gestao_atendimento_filas_espera>

DeepSearcher, Inc 2012. Chapter 18: Threats, Attacks, Hackers & Crachers. Downloaded April 12, 2012. <http://www.intelligentedu.com/computer_security_for_everyone/18-threats-attacks-hackers-crackers.html>

Desmond, Paul 2004. All-out blitz against Web app Attacks. Downloaded April 15, 2012. <http://www.networkworld.com/techinsider/2004/0517techinsidermain.html>

Equinux AG and equinux USA, Inc 2010. VPN Configuration Guide, Cisco ASA 5500 Series. Downloaded April 11, 2012. <http://www.equinux.com/cms_components/media/vpnt/VPNT_Interop_Howtos/1101/CiscoASA.pdf>

EVT Solutions, Inc 2009. Reach More Customers. bLoyal enables you to effectively manage your product catalog, pricing and inventory in one place. Downloaded

March 12, 2012. <http://www.bloyal.com/Solutions/ValueProposition/ReachMoreCustomers/tabid/63/Default.aspx>

Face to Face.com 2010. Start, Product. Downloaded March 12, 2012. <http://www.face2facekiosk.com/>

Hentea, Mariana 2012. Informaiton Security Management- OVERVIEW, SECURITY THREATS IMPACT, EMERGING SECURITY THCHNOLOGIES, SOLUTIONS, SEMMODEL REQUIREMENTS, CONCLUSION. Downloaded April 12, 2012. <http://encyclopedia.jrank.org/articles/pages/6625/Information-Security-Management.html>

Hewlett-Packard, Development Company 2011. Disaster Tolerant and Continuous Computing. Downloaded March 12, 2012. < http://h71028.www7.hp.com/enterprise/cache/197861-0-0-225-121.html>

Information Security Plan 2011. INFORMATION SECURITY PLAN. Information Security Board of Review Members. Michigan Technological University. Downloaded April 4, 2012. < http://www.security.mtu.edu/policies-procedures/ISP_Final.pdf>

Kimberly, Graves 2007. CEH: Official Certified Ethical Hacker Review Guide. Downloaded March 22, 2011. <http://books.google.fi/books?id=1yj97C_K_zAC&pg=PA121&lpg=PA121&dq=a+lot+of+system+resources+are+occupied+at+the+same+time++DDoS&source=bl&ots=oAlDeAR5XU&sig=mfIcXch0Nt1614bddxNL2tUy8k4&hl=zh-CN&sa=X&ei=T2SRT-DOBaqp4gS-oL3EBA&ved=0CDYQ6AEwAg#v=onepage&q=a%20lot%20of%20system%20resources%20are%20occupied%20at%20the%20same%20time%20%20DDoS&f=false>

Kroll Ontrack, Inc 2012. File Recovery Software. Downloaded April 12, 2012. < http://www.krollontrack.com/data-recovery/recovery-software/>

Kuinam, J Kim & Seong, Jin Ahn 2011. Proceedings of the international conference on IT convergence and security 2011. Downloaded April 18, 2012. <http://books.google.fi/books?id=JxyB_p1g6uMC&pg=PA106&dq=the+steps+of++DDoS+attack&hl=zh-CN&sa=X&ei=N5yZT-DRG7PU4QTxn-XEBg&ved=

0CEAQ6AEwAw#v=onepage&q=the%20steps%20of%20%20DDoS%20attack&f=false>

Lin, P Paul 2009. System Security Threats and Controls. Downloaded April 13, 2012. < http://www.nysscpa.org/cpajournal/2006/706/essentials/p58.htm>

QuinStreet, Inc 2012. Firewall. Downloaded April 19, 2012. < http://www.webopedia.com/TERM/F/firewall.html>

QuinStreet, Inc 2012. RAID. Downloaded April 19, 2012. <http://www.webopedia.com/TERM/R/RAID.html>

RAID Data Recovery 2006. Advantages and Disadvantages of RAID. Downloaded April 14, 2012. < http://www.raid-data-recovery.net/advantages-raid.html >

RTC Group, 2008. Products & Technology. Downloaded April 19, 2012. <http://www.rtcmagazine.com/articles/view/101023>

Security Awareness 2010. Firewalls: What They Are, What They Can Do for You. Downloaded April 14, 2012. < http://www.utexas.edu/its/secure/articles/firewalls.php>

Smith, Bradford 2008. Hacking the Kiosk Managing the Risk of Public Information Systems. Downloaded February 2, 2012. <http://www.mcafee.com/us/resources/white-papers/foundstone/wp-hacking-kiosk.pdf>

Thomas, Charles E & Lee, Minyoung & Bedard, James F & Hayashi, Steven R & Harris, Lawson P 1988. Vibration-sensing tool break and touch detector optimized for machining conditions. Downloaded April 18, 2012. <http://www.google.fi/patents/US4724524?printsec=abstract&dq=characteristic+of+digital+vibration+sensor+detector#v=onepage&q=characteristic%20of%20digital%20vibration%20sensor%20detector&f=false>

Toffler, Alvin 2011. BrainyQuote.com. Xplore Inc. Downloaded April 18, 2012. < http://www.brainyquote.com/quotes/authors/a/alvin_toffler.html>