KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES

Infrastructure Plan for Home Security System

Tong Yao

Bachelor's thesis of the Degree Programme in Business Administration

Business Information Technology

Tornio 2011

CONTENTS

ABSTRACT

Tong, Yao. 2011. Infrastructure Plan for Home Security System. Bachelor's Thesis. Kemi-Tornio University of Applied Sciences. Business and Culture. Pages 53. Appendix 1.

The aims of this research were to design an infrastructure plan for home security system, analyze the most mature and emerging technologies, connect the security services through different types of interfaces, and assign different security levels for home security system based on the user requirements. The whole infrastructure plan could be used as a handbook that a user can consider to tailor the home security system.

Various devices and their handbooks for home users to construct their home security system exist in the market, but they are separate and fragmentary. Moreover, to install each device together via different types of interfaces, ports, or protocols is challenging for a home user. Those reasons above triggered me to make an infrastructure plan for a home security system. The beneficial users are the people who have a demand to build a secure home security system, or the one who have interests in the home security system.

Constructive method have been the mainly methodology throughout the work. I was seeking a practical and new solution based on past studies. The techniques contain interview, questionnaire, and literature analysis. I was looking for a better understanding of user requirements and the background information of computer based or network based home security systems.

The expected output was a plan for an integrated security system that is easy to setup, convenient to configure, and flexible to use. The infrastructure plan for a home security system can be implemented in future when the technology of devices is mature enough.

Keywords: Infrastructure Plan, Home Security system, Information Security Management

FIGURES

PICTURES

1 INTRODUCTION

In Microsoft Security Intelligence Report (Shostack et al. 2009, 14), it is suggested that the top data loss threat continued to be stolen equipment such computers, which accounted for 30% of reported data loss incidents. This statement indicates that in the current situation, home security is increasing its value for people to research. Since home networks are easily exposed to vulnerabilities, supervisory control of residential environments has become increasingly important by network computers or even through mobile devices.

Technologies are developing all the time. Although different devices and their handbooks for home users for their home security systems exist in the market, they are often separate and fragmentary. Users are often confused about the various devices in the market. It is also a challenge to install them together through several types of interfaces, ports, and protocols. To remember different pin-codes causes a headache.

From the network infrastructure's point of view, to specify different security levels is essential because different user groups may have different requirements. Unifying the different security levels is still a blind angle in today's market (Meriläinen 2010).

The problems above triggered me to consider an integrated home security system and its guideline that is under the users' control. Moreover, costs of devices for the wireless system should be concerned on the ordinary consumption level of consumers.

Basically, the home security system is includes

- Wired and wireless network
- Backup device, e.g. Apple Time Capsule
- Web-Camera monitoring system (movement detector)
- Electric locks
- Alarms (mobile phone, e-mail) warnings
- Other security devices.

For a home network, a mixed wired and wireless network is engaged in the system to achieve a flexible network topology, and lower the cost for the user. Backup device such as Apple Time Capsule is a wireless network-attached storage device, which can be used to back up files or a system automatically (Apple 2009). Apple Time Capsule backup device is also possible to be attached by an external drive or printer. Web camera can be connected to a home computer so that the image it monitors can be presented and saved on the home computer. Alarm warnings and electric locks are considered as a part of the whole wireless system that refers to different levels of security. Usually, service providers, such as Sonera, Elisa and DNA in Finland, are support the services of the device and maintain the device they offered. In this thesis work, the service provider should be accountable in terms of authentication, authorization, identification, and integrity to the services in case of an emergency. However, numerous service providers are increasing the complications of the users' usability if parts of the home security system are breakdown (Interview 2010).

Advanced devices are as follows:

- Radio-frequency identification（RFID）tags
- Barracuda security card.

Radio-frequency identification（RFID）tags are about devices and technology that use radio signals to exchange identifying data (Lindstrom & Thornton 2005, 4). Concerned about the home security system, it can be applied to track all the vital equipment within a home range and all the information will be recorded in the home computer. In the thesis work, the usability of RFID tags, and their future functions are both analyzed.

Barracuda Anti-theft device, i.e., the CUDA Card, which is installed in computer, is used to protect the computer from theft and tampering by using an ambient light sensor. This device, shows in picture 1, sends an alarm which sounds for a period of one second if an accidental movement occurs. (West Coast Publishing 1999). Because of the cost（Around 140 Euros）and the sensitive level of the personal data, the CUDA card could be an optional choice for the design of the advanced level.

Picture 1. Barracuda security card

In general, the thesis work was aimed to provide an infrastructure plan for home security system, which could be achieved by analyzing the most mature and emerging technologies of home security system, studying the interfaces and ports of the devices, and assigning the security level based on the user requirements. It was also aimed to be an introductory and a referential guideline for a home user during the home network security system construction.

The structure of this thesis is as follows. The main research question is presented in Chapter 2. Methodology is introduced in Chapter 3. In Chapter 4, the reader can find the general information of home security system, and a comparison among different types of home security systems. Chapter 5 is focus on the beneficial user of this thesis and user requirements of computer or network based home security system. An analysis of network connection, network connectivity devices and devices interfaces are described in Chapter 6. Usability and the implementation of the infrastructure plan for a home security system, is depicted specifically in Chapter 7 and Chapter 8. Chapter 9 reviews the future development as well as summarizes the results of the research.

2 RESEARCH QUESTION

The process of collection and analysis of the user requirements was the foundation of the infrastructure system plan. The general functions for a home security system include protect, monitor, detect, and alarm the normal activities in the residential environment, especially when an incident or incidents occur. The infrastructure plan was also contained the defective and protective mechanism for security sensitive level that user needs to have (Meriläinen 2010). The following research question was concerned to fulfill these goals.

What kind of architectural solution is appropriate to combine different home security sub-systems together so that the whole system is fulfilling the requirements of usability, safety, and security?

A different user requirement was an indispensable factor under the consideration of designing the infrastructure plan for the security system. A different user requirement was also referred to the various levels of usability, safety, and security services. Moreover, the integrity system was involved in both basic and advanced level to meet different needs of a user. An infrastructure plan was formed in order to process a home security system. Users could select the security level that fits their own home security requirement.

To be specific, the basic level of the home security system should contain the fundamental wireless devices, such as: router, computer, backup devices, electric locks, web camera, and alarm warning device. The advanced level should include Radio-frequency identification (RFID） tags and Barracuda security card, in addition to the devices in the basic level. Evidently, it is not a compulsory requirement for each level; users can choose devices flexibly, or even connect more devices based on their requirements.

The architectural solution of a home security system contains physical and logical topology and available interfaces of each device. In addition, a suggestion of wired or wireless network that is suitable for the home users' requirements is also taken into

consideration. The solution might be partly practical because of the limitation of the present technologies. However, it is still valuable for a home user to consider their home security system. One typical solution is offered in Chapter 8. The outcome of this infrastructure plan for a home security system is possible to connect with different security subsystems to form an integrated security system. Furthermore, it is easy to setup, convenient to configure, and flexible to use.

3 RESEARCH METHODOLOGY

Constructive research is the main method of this paper. Questionnaires were used to collect the information necessary for the design of the home security system. Moreover, literature analysis was applied to make the best option of the infrastructure plan for a home security system as well as to facilitate the future development of the interfaces for each devices within the system. In addition, interviews have been taken in order to understand the attitude of the present home user facing home security and the developing direction of today's home security devices.

Constructive method aims at producing novel solutions to practically and theoretically relevant problems (Hair J et al. 2007, 179-222). This method also builds an artifact that solves a domain problem in order to create knowledge. Because of the aim of my research was to make an infrastructure plan for a home security system, various user requirements should be identified and analyzed. Besides, my thesis seeks to provide a practical and new solution to a classified network infrastructure that builds on past studies. Hair J et al. (2007, 179-222) state that "constructive method is about how the problem can be solved and if previous solutions exist, how the solution is new or better than previous ones".

According to Hair et al. (2007, 179-222), the phases of constructive research are as follows:

1. Find a practically relevant problem
2. Obtain an understanding of the topic and the problem
3. Innovate, i.e., construct a solution idea
    - Heuristic process
    - Theoretical justification and testing come later
4. Demonstrate that the solution works
5. Show theoretical connections and research contribution
6. Examine the scope of applicability.

Based on the list above, the first stage of my research was to access and to analyze the user requirements on the home security. The next step was to classify the gathered

information into two security levels: basic and advanced. The procedures of constructing the devices within a network system were also carried out. The final step was to verify the full functions of the system in terms of the effectiveness and the flexibility of the whole system.

Interview, questionnaire, and literature analysis were the supplementary research techniques used in the research. Interviews provided an insight into the specifications of the real-world system, and offered a practical foundation of the research as well. The staffs from Lukko Oy in Tornio Finland and from a shop named Gränslås in Haparanda Sweden were interviewed. The interviews were intended for gathering the information about the present home user orientations on home security devices and the existing home security devices in the market.

The choice between two formats of questions was considered, i.e. structured or open. The latter type was selected to avoid structured responds and to collect more ideas which assist to form an infrastructure plan for a home security system. The target group for answering the questionnaires was the students and teachers from Kemi – Tornio university of Applied Science, home security devices sellers from Finland and Sweden. These groups were chosen because the general home user of the home security system was towards each individual or families who had willing or interests to install home security devices. Different specialty and various working background of people were required to get an outcome and a suggestion of the future improvement. Also the questionnaire was an efficient way to collect relevant information from many respondents for the design of the home security system.

The research ran through conducting a literature review. Collection and analysis of the relevant information was formed from books, articles, and the Internet. The literatures to be reviewed were the information on home security system and information system management. The purpose of literature review was to convey what knowledge and ideas had been established on the topic. The literature review had to be defined by a guiding concept, such as the research objective, the problem or issues discussed, or the thesis argumentation (Taylor 2009).

4 BACKGROUND INFORMATION OF HOME SECURITY SYSTEM

4.1 General features of home security system

Information that acts as the lifeblood of human beings is influencing us in our daily lives. Besides, the existing home security systems are separate and fragmented, which was the most essential factor to form an infrastructure plan in order to construct an integrated home security system. It is also beneficial to study the interfaces of different systems so that it is possible to know how they can be connected together.

One feature of the integrated home security system is that the system will be constructed with detection technology, such as sensor and detector. The advantage on miniaturization techniques and wireless communication make possible the creation and subsequent development of the residential network paradigm. The main purpose of the home security system is to serve as an interface to the real world, providing physical information such as temperature, light, and movement detection to a computer system. The major difference between this type of networks and wired networks is the decentralized and specialized. The components of the home integrated security system collaborate towards the common goal of obtaining or deducing certain physical information from the surrounding, and to be able to realize the self- organization without requiring the existence of a supporting infrastructure.

The devices that have been listed above for various levels of home security system were partly available in the practical part of the research such as router and computer. The web-camera could be possible to present later on. It is not necessary to master all technologies since technological solutions can be grouped together (Purser 2004, 23-25). Even though lack of devices was not affecting the realization of the infrastructure plan for home security system in this thesis work, the basic network is possible to build up only with cable, router and computer. Other devices act as modules that can be inserted into the system afterwards. It was possible to make the plan of the entire system via the materials that are available at the library, the Internet, and the assistance from the thesis supervisor.

4.2 Benchmarking different home security systems

According to the interviews of two shops on 4 October, 2010, one is Lukko Oy in Tornio, Finland; the other is called Gränslås in Haparanda, Sweden, Network based or computer based home secure system has not been launched in the market in Finland and Sweden yet. The introduced home security system in Finland and Sweden are a combination of home security devices with a GSM based remote control. GSM based remote controlling system is a system that sends emergency calls to a monitoring company by a phone. The alarm is triggered by a sensor, or other devices within the living environment. The phone number has already been bound to your home security system before it is taken into use. The most serious problems are fake messages. They will be sent without the notices of a home user and they lead to the wastage in terms of human, material and financial resources. This situation may happen unassumingly e.g. the telephone's keypad is not being locked. (Interview 2010).

Computer or network based home security system, as name implies, is a home security system being built based on network through the control of a computer, combined with various sensors via a control panel. The control panel that acts as a central control device allows home users to specify both the menu path and the module. In several circumstances, the control panel modules recursively build sub-panel under the main control panel.

The computer or network based system design is not negating the GSM based home security system. Adversely, it is a supplementary way of the control of home security system, and acts as the other option for a home user. A computer or a network based system must work under the Internet connection that is similar to GSM based system, but takes action by mobile phone.

The functionality and behavior of the computer-based home security system is also different from another network paradigm, Mobile Ad Hoc Network (MANET). First, all devices in computer-based home security system are almost autonomous; with little interfere by human users. Secondly, those devices are much more constrained in terms of battery life and processing power, so it can only offer a simple and predefined set of tasks, whereas a MANET node is usually a PDA-like device with much more functionality and resources. In addition, the density of computer-based home security system is usually higher than MANET. (Lopez & Zhou 2008, 1).

The function is similar to a wireless sensor network (WSN) to a certain extent. According to Lopez & Zhou (2008, 1-3), the major elements of WSN are the sensor nodes and the based stations. WSN can be abstracted as “sensing cells” and the “brain” of the network. Respectively, Sensor nodes get the physical information of the surroundings using its built-in sensors, process the raw information taking advantage of its computational capabilities, and communicate with other nodes in its surroundings using a wireless channel. All sensor nodes are battery-powered; hence, totally independent and able to operate autonomously. All data coming from the sensor modes, as well as all control commands that can be issued to those nodes, will traverse the base station. (Lopez & Zhou 2008, 1-3). The mainly difference, compared with home security system, is a home security system can be functioned as either a wired or wireless network.

The following picture presents several of the devices in Lukko Oy where the interview was implemented. The devices are different kinds of movement detector, Web-camera, smoke sensor and IR (Infrared Ray) detector.

Picture 2. An interview in Lukko Oy in Tornio, Finland

5 USER REQUIREMENTS OF HOME SECURITY SYSTEM

The beneficial users of the whole system in this paper are the people who have a demand to build a secure home system, or those who need to reconstruct their existing home security system. The infrastructure plan for home security system is also oriented to those who have interests in home security system. Teachers, students from Kemi-Tornio University of Applied Sciences, and sellers of security devices have been interviewed.

5.1 Viewpoint of general home user

A general home user of a computer or a network based security system is mostly the one who has willing to install home security devices. The present situation is that users do not have a keen demand to install in advance an integrated security system. The numerous user requirements are concentrating on the basic security needs, such as door lock, smoke sensor, etc. A few home users have interests in advanced home security level, except those related experts, amateur, or those who have especial residential security needs.

The general home users usually have little experiences about the installation and the maintenance of the security devices. They also have problems in the selection of products and devices. They are even lacking a clear understanding of the appropriate price of a specific product. Therefore, the general home users trust on the opinions of the service provider and the product seller.

The average costs of the devices that the general home user will afford are between 1000 and 1500 Euros. Most of them are willing to receive assistance within 15 minutes and a service delay within 1 minute. Besides, the best way for them to control the whole system is via a keyboard.

5.2 Viewpoint of relative experts and seller

The relative experts are the people who have experiences in selection, installation and

maintenance of the home security devices. They usually have interests on installing home security system; however, less than 50% of experts take actions due to the high cost of home security devices, which indicate that the expert occupied a miniature scale of the whole home user group.

The average expense on the devices that the experts spend is between 1500 and 2000 Euros, is slightly higher than a general home user. A dominant part of them choose to receive assistance within 10 minutes and a service delay within 1 minute. If a connectivity problem occurs, they will try to solve it firstly by themselves, and secondly look for help from the service provider if the solving process is unsuccessful. Besides, the best way for them to control the whole system is via a keyboard, which is similar to the choice of the general home user.

The sellers of home security devices are those who are familiar with the home security devices. Since the general home users have rarely made a research on the home security devices by themselves, the information is practically generated by the seller of the devices. According to the interview, some of the advanced home security devices have already been unloaded in the current. However, this situation may not last in future as long as the overall home secure environment is worsening, even though it is not an optimistic sign.

5.3 Discussion

According to the results obtained from the questionnaires and interviews, it became obvious that the there is a need for infrastructure plan for home security systems. The infrastructure plan for home security system is offered a solution based on the requirement of the general home users in Chapter 8.

6 NETWORK DEVICES AND INTERFACES ANALYSIS OF HOME SECURITY SYSTEM

6.1 Network connection and connectivity devices analysis

A network is two or more computers that are connected with a communication line for a purpose of sharing resources (Gilster & Ron, 2002, 510). Figure 1 illustrates a basic network that connects Tom's PC to Sally's PC so that they can share each other's file. If two or more computers connected to each other over a telephone line or cable and peripheral devices on the other computers, a network is formed.

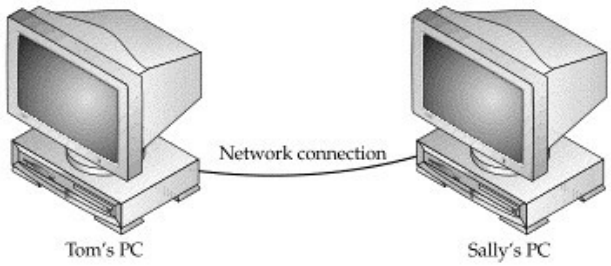


Figure 1. Peer-to-peer networks (Gilster & Ron, 2002, 510)

There are two basic network structures: peer-to-peer (peer-based) networks and Server-based (client/server) networks. Peer-to-peer networks are two or more computers directly connected to one another for the sole purpose of directly sharing data and hardware resources. (Gilster & Ron, 2002, 511). Figure 1 is a typical example of peer-to-peer network. Server-based networks are referring to the network of connected computers and peripherals with a centralized server that facilitates the sharing of network data, software, and hardware resources (Gilster & Ron, 2002, 511-512). Figure 2 indicates the centralized management of a server-based network. With server-based network, the permission and access to the networking resources are controlled by a central administrator. In general home network, since the users of computer are limited, peer-to-peer network is usually be involved in.

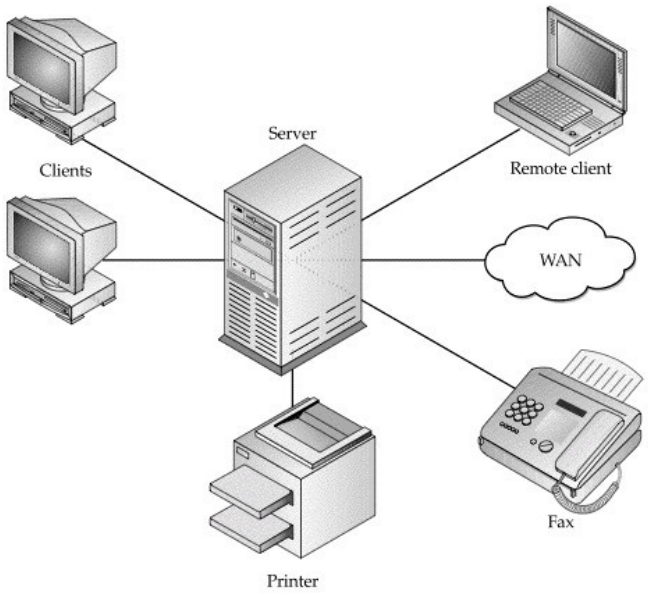


Figure 2. Server-based networks (Gilster & Ron, 2002, 512)

According to Gilster & Ron (2002, 513), the most basic network components are servers, workstations (computers), and other network nodes (printers, modems, etc.), the network operating system (NOS), and the cabling or media used to connect them all together. The easiest way to share a communication link on a home network is through a network connectivity device. The basic network media include repeater, hub, bridge, switch and router. (Gilster & Ron 2002, 513).

A repeater is used to regenerate the signals and retransmit it in order to gain the signal when a network devices at a distance that exceeds the maximum segment distance. The maximum segment length limited on a network medium includes all pieces of cabling between the signal source and the destination device. (Gilster & Ron 2002, 521).

Both a hub and a switch are exchange points in an Ethernet network. Hub, serves as a clustering device that allows several devices to interconnect to the network and each other. In a home networking environment, a hub is used to cluster two or more computers or peripheral devices to the residential gateway devices. Such as the one shown in Picture 3, a hub is a link to several computers and peripheral devices, which creates a small peer-to-peer network. A bridge is used to interconnect two dissimilar network segments, such as an incoming DSL link and the local network. (Gilster & Ron, 2002, 521-522).

Picture 3. An eight port Ethernet hub

A switch performs the hybrid function as a hub and a bridge – it connects the nodes of a network to one another, but rather than sending every packet, a switch reads the address section of each incoming packet and sets up a direct connection from the source of each packet to its destination (Ross, 2009, 30). A switch is present in the Picture 4 below. In general, hubs are slow, simple, and cheap, whereas a switch is more efficient than that of a hub; especially the efficiency of the network bandwidth is improved.

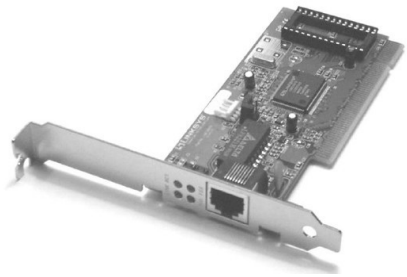
Picture 4. An eight port Ethernet switch

According to Gilster & Heneveld (2004, 230), a router is the workhouse of high-speed communication connections. It is embodying all the functionality of hubs, bridges, and switches and performs a very valuable service as well –routing. Routing is the process that forward messages from the local network to a remote network, such as the Internet. The aim of routing is to forward a message alone the best path possible to reach its destination. On a home network, the message is transmitted either inbound or outbound directly to the router port where a particular home network workstation is located. Picture 5 is an outlook of a wireless router. A wireless router can enable both functions of wired or wireless network, which makes it to be a better choice of a home networking.

Picture 5. A wireless DSL Internet gateway router

6.2 Interfaces analysis of home security devices

Network interface devices (NIC), or network adapter, is the devices that connects computer to a network. The PC interacts with the network and its resources through the NIC (Gilster & Heneveld, 2004, 217). Network interface device is designed in a variety of styles. Referring to Gilster & Heneveld (2004, 217-218), the most common type is an expansion card, which is installed in an expansion slot on the PC's mother board, shown in Picture 6.



Picture 6. A PCI (Peripheral Components Interconnect) network interface card (NIC) expansion cards

The expansions card NICs works for both wired and wireless networks, while the difference is that there is an antenna in wireless NIC (Picture 7), which connects the NIC's transceiver to a wireless network access point (NAP) and the network.

Picture 7. A wireless NIC expansion card (Photo courtesy of Cisco System, Inc.)

Most of today's network expansion card NICs are typically designed for installation in a PCI (Peripheral Components Interconnect) slot on a computer's motherboard inside the

PC's case as Pictures 6 & 7 presents. The "legacy" computers provide older interface types as ISA (Industry Standard Architecture) interface. There are also computers using EISA (Enhanced ISA) slot, a combination shot that can wither a legacy ISA card or an EISA card. (Gilster & Heneveld 2004, 217-218).

Portable PCs, such as notebook and laptop computers, are typically using PC Card network adapters. Some portable PCs have a network adapter built into the motherboard; in this case, a connecting Jack is available on either the case of the PC or its Docking station. A PC docking station is a platform where a notebook PC can be mounted to gain additional ports, jacks, and a network interface. (Gilster & Heneveld, 2004, 217-218). A network adapter of a portable PC is shown in Pictures 8 & 9.

Picture 8. A notebook computer with a PC Card network adapter installed

The NIC shown in Picture 9 is a PC card adapter that user a dongle to connect to the network media (Gilster & Heneveld, 2004, 218). There is a jack in the end of the dongle.

Picture 9. An Ethernet PC Card (PCMCIA) type network adapter and a dongle connector

The network NICs or adapters above are using a physical wire or cable to interconnect

computers and other devices to the network. While a wireless NIC, such as the one in Picture 10, is distinctive with its radio frequency (RF) antenna on the external part of the expansion card (Gilster & Heneveld, 2004, 220). As wireless connection is popular and convenient for home user, compared with a wired network, it also can be integrated into a control panel by central control. Wireless network connection is one of the preliminary components within the home infrastructure plan in this thesis.

Picture 10. A wirelesses PC Card network adapter (Photo courtesy of Cisco System, Inc.)

A USB (Universal Serial Bus) network interface is another type of wireless NICs. It can be hot-installed at any time, whether the computer is running or not. (Gilster & Heneveld, 2004, 219-222). Picture 11 presents a USB network NIC that is connected to the PC using a USB cable.

Picture 11. A USB (Universal Serial Bus) network NIC (Photo courtesy of Cisco System, Inc.)

The most widely used types of USB NICs, is presented in Picture 11 & 12. A jack is used to connect to the network Media through the USB port.

Picture 12. A wireless desktop USB network adapter (Photo courtesy of Cisco System, Inc.)

The Newer generation of USB NICs is available to connect directly into the USB port, shown in Picture 13. Newer and more compact USB network adapters are now available to connect to the USB port directly (Gilster & Heneveld, 2004, 220-221).

Picture 13. A compact USB network adapter connects directly into the USB port on a PC (Photo courtesy of Cisco System, Inc.)

Network connection can also be achieved through power-line or phoneline wiring already in a home. These systems require special types of network adapters, shows in Picture 14 below.

Picture 14. Power line control (PLC) Network adapter (Photo courtesy of Net Gear, Inc.)

In General, concerned about a majority of today's expansion card NICs and the compatibility with the legacy computers, PCI is a better option for its popularity. If

home users have more notebook or laptop computers, the PC card network adapters are a better solution. The USB network adapter can also be taken into consideration for its hot-installed in wireless network connection.

The selection of the Network interface was determined by the architecture of the home security system in the thesis. The infrastructure plan has emphasis on the central control of a home security, which can hardly be realized only via the wired network control. Under the circumstance of a highly controlled and monitored home security system, a large number of wireless and wired devices need to be adopted. The reasons above elicited the importance of interface analysis, with which, the most popular, precise interface card could be chosen and be inserted into the devices. Furthermore, the devices which do not have a slot for the network interface card at present, such as sensor, can also be taken as a reference for the future design and installation.

7 PRELIMINARY DESIGN OF HOME SECURITY SYSTEM

7.1 Classification of Home network

Home network types are described as data network and control network, in general. Data network is the networks that use the signals to transmit between the computers. Data network represent various forms of data, including text, graphics, and sound signals encodes in digital/ data form. The control network (also called home automation networks and home technology integration networks), depicted as the prime type in this thesis, is used to manage and control lighting, heating, ventilating, air conditioning (HAVC), appliances, and home security systems. By eliciting the perspective from Gilster & Heneveld (2004.203), control networks use computer-based controls and receivers. The controller transmits commands and control data across the network to the receiver, which either acts on the incoming data or retransmits to another device, such as an appliance, stereo, light fixture, or whatever has been attached to the network for automation purposes. In brief, a control network is used to control, monitor, and manage one or more of a home's system. A typical example of a home control network is the heating and cooling system and a thermostat. Or an indoor light system regulated by the outside controller, as well as the scheduled events the users wants to trigger. (Gilster & Heneveld, 2004, 203).

The basic network, illustrated in Figure 3 below, consists of a few primary components: computers, network adapters, cabling, and if required, some form of network clustering or connectivity device. The network in Figure 3 is connected by a communication device – modem to share a connection within a residential environment to an Internet service. The modem can also be a residential gateway device.

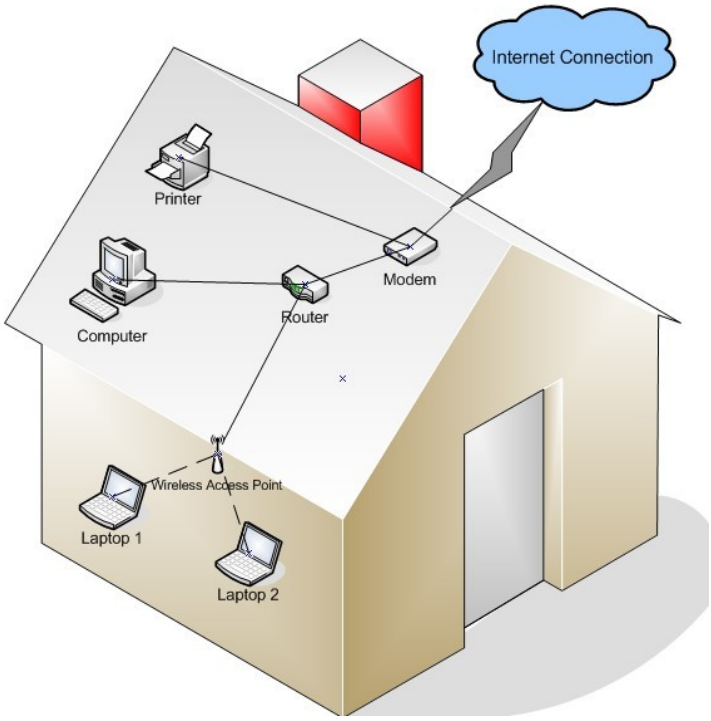


Figure 3. Physical layout of a simple home network

The only difference between the home computer network and other types of computer network is the scale. A home computer network can be as simple as two PCs connected by a medium, a printer, for instance, to share files, or internet connection. A home computer network can be very complicated and sophisticated as a lighting system, heating and cooling system, security system which is being controlled and monitored by a central control panel. However, a business computer networks can be a net of computers and network devices depends on the company's size and its physical layout. More often than not, a home computer installed for the purpose of sharing internet connection and its resources in a home. The importances of home networking are listed as follows (Long, Larry 2002, 16):

- Share broadband Internet access
- Share files among PCs on the network
- Share printers and other resources
- Integrate home entertainment and personal computing
- Play multiplayer games
- Enhance PC and network security
- Go wireless with PCs and other devices
- Create an e-home

7.2 General architecture plan of home security system

The general architecture plan of this thesis was designed based on the network through the control of computer, combined with various sensors via a control panel. The control panel, acts as a central control device, allows home user specify the menu path and also the module. In several circumstances, the control panel modules recursively build sub-panel under the main control panel, which could be present in Figure 4:

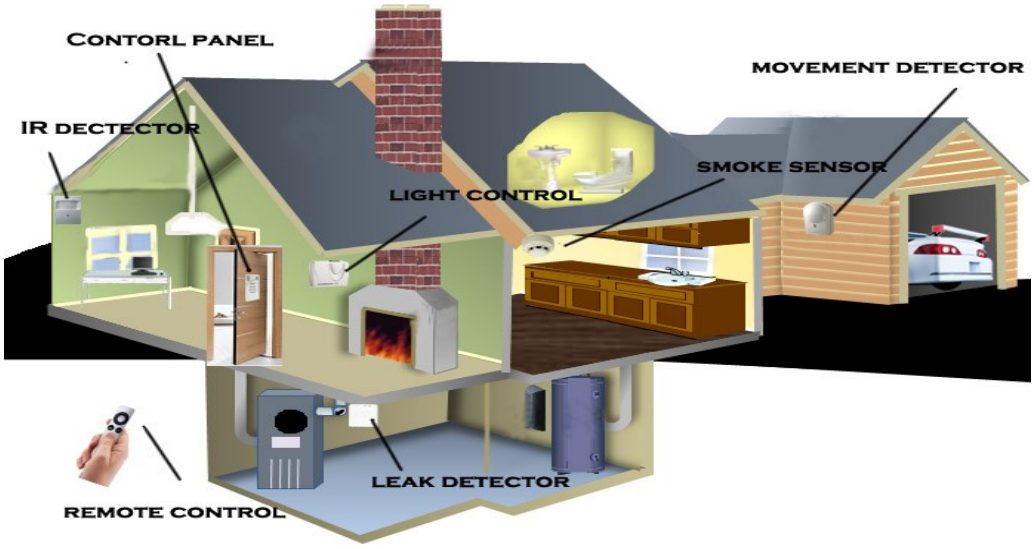


Figure 4. Home Security System with Control Panel

Figure 4 presents kinds of detectors and sensors as sources of control panel. The detectors and sensors take control of lights, energy leakage, smoke, movement, etc. Besides, a remote control is used straightforward the control panel. All listed functions are merely the examples of remote control; accordingly, a home user can make options that depend on the needs of their own.

Considered the part of the computer based or network based devices, these devices should include wireless interface cards so that they can be integrated into the whole system and realize the central control. With a central control, a home user can simply monitor their residential environment using the laptop, Mobile phone or any other devices through Internet connection. An obvious limitation using GSM based system is that a home user can call only for urgency to a remote company that takes actions that are needed in the situation when no one is at home. A network based system conquers it. With network connection, home users are assisted by another way to control their home

environment. It is also possible to make the monitoring image visible from monitoring screen through a webcam.

The types of Internet connection are Dial-up, Satellite, Cable, ISBN (Integrated Services digital network), DSL (Digital Subscriber Line), T1 or wireless or other high speed connection. The most common network connections are cable Internet connection and ADSL (Asymmetric Digital Subscriber Line) Internet connection. (Coleman & Stephen 2000, 10). For each type of the Internet connection, there are several network layouts and the network devices to support the Internet connection.

Relied on the perspective of Petri (2009), there are several approaches to set up a home network, or SOHO (Small Office Home Office) network through ADSL (Asymmetric Digital Subscriber Line) Internet connection. ADSL is a high-speed Inter access service that utilizes existing copper telephones lines to send and receive data at speeds that far exceed conventional dial-up modems (R. Kayne 2010). The first option is to connect all the required devices and Ethernets cables through a hub or switch. The hub or the switch can be any model UTP (Unshielded Twisted Pair- a regular copper wire) based hub preferably with either an uplink crossed connector or a UTP crossed-over network cable. The hub should be equipped with at least 1 ADSL UTP Ports. The layout can be specified in Figure 5 below:

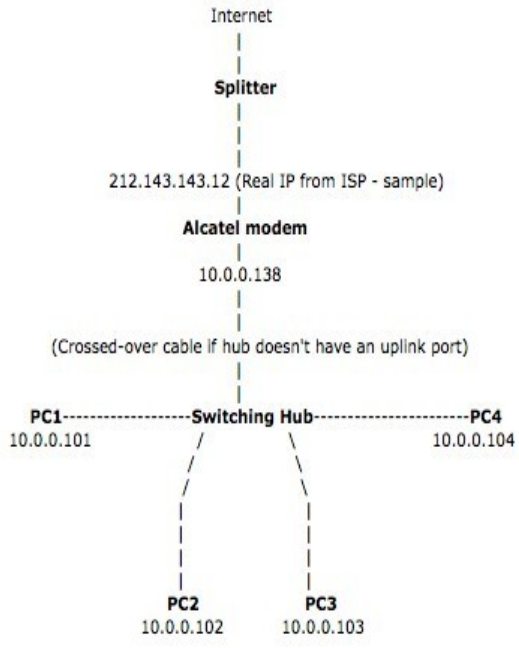


Figure 5. Network setup layout 1 (With a hub or switch)

An ADSL cable is inserted into splitter which is connected with an ADSL modem. Splitter is a device that divides a telephone signal into two or more signals, each carrying a selected frequency range, and can also reassemble signals from multiple signal sources into a single signal. (Tech Target 2010) For ADSL, the splitter divides the incoming signal into low frequencies to send to voice devices and high frequencies for data to the computer. The Ethernet cable from the modem can either be connected to the uplink UTP connector of the hub, or to a regular UTP connector using a UTP crossed over cable. Each PC should be linked to a regular UTP port of the hub or the switch with a unique IP address. (Petri 2009).

This type of network connection is simple to setup and no server is needed. Also the configuration of each PC is manual. But merely 4 PCs are allowed to link to the hub or switch with a fixed IP address. And only one PC at a time can be connected to the Internet. It is still beneficial to the limited home user nonetheless. (Petri 2009).

The second option is similar to the first one, except that one PC is used as a server, which enables to utilize a different IP range from the one offered by ISP (Internet Service Provider). (Petri 2009). It is states in Figure 6 as follows:

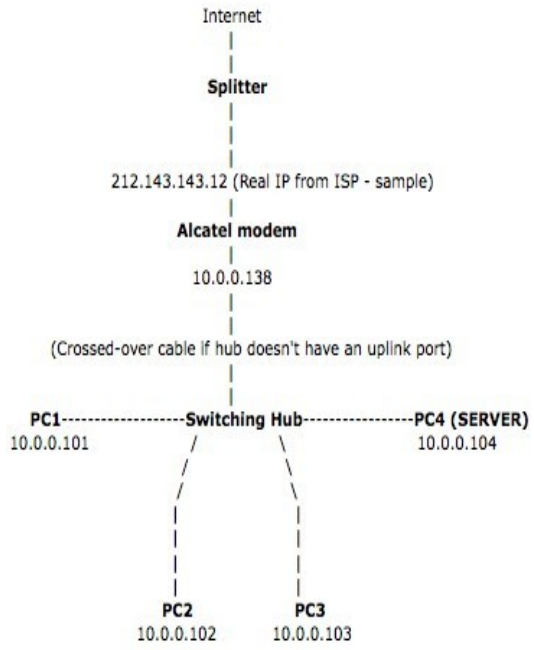


Figure 6. Network setup layout 2 (With one computer act as a server)

The process of the Ethernet cable and the network devices are similar to the layout 1

specified above. One distinguished step is that one PC is required to be configured as server using software such as WinRoute or Microsoft Internet connection Sharing (Windows 2000, XP and ME have this standard included). (Petri 2009).

The foremost advantage of layout 2 is that one PC acts as a server so that there is no limitation of the numbers of PC to be using, as long as there are still spaces for assigning IP address (254). Besides, dial up is done automatically and no manual PC configuration is required. Likewise, the disadvantage is that the configuration of the server can be difficult. (Petri 2009).

The third method for home network setup is achieved by a server connected to ADSL. This layout is similar to the option 1 and option 2 except that an ADSL cable is connected to a server directly and for that server a second network connection is connected to a hub or a switch. There are no limitations of hub and switch to the user. The third method of networking can be functioned as a hub-free network. Moreover, the configuration of PC is automatically. To enable this type of network connection, the server should have two network cards available. One is for ADSL connection, the other is for the connection of LAN/Hub. LAN refers to Local area network. (Petri 2009). The network layout is shown in Figure 7:

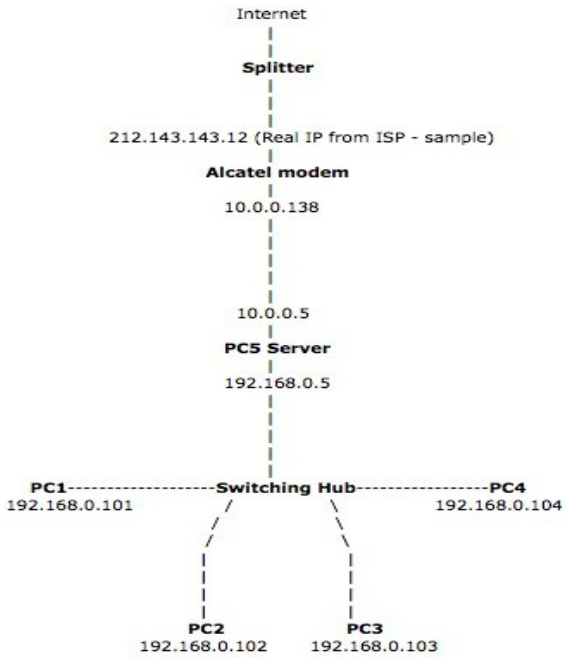


Figure 7. Network setup layout 3 (server directly connected to ADSL)

An ADSL cable goes to a splitter. An ADSL modem is connected to the splitter. An Ethernet cable link the connection between the modem and a PC Server. The second network card of the server is connected to a hub. Finally, each PC is connected to a regular UTP port of a hub or a switch.

The fourth way to setup a home network is through a connection from PC and ADSL to a router or a switch, which is visible in Figure 8 below. The router or the switch acts as both a server and a hub in a network. The user benefits from the simple setup and auto-configuration of a PC. Its advantage also covers the aspects of separation between the Internet and the LAN, and no requirement of a PC. But the Router can be expensive and hard to configure. (Petri 2009). Moreover, not all the ADSL routers support PPTP (Point-to-Point Tunneling Protocol), a networking technology that supports virtual private networks (VPN), enabling remote users to access corporate networks securely (Bruin Online, 2009).

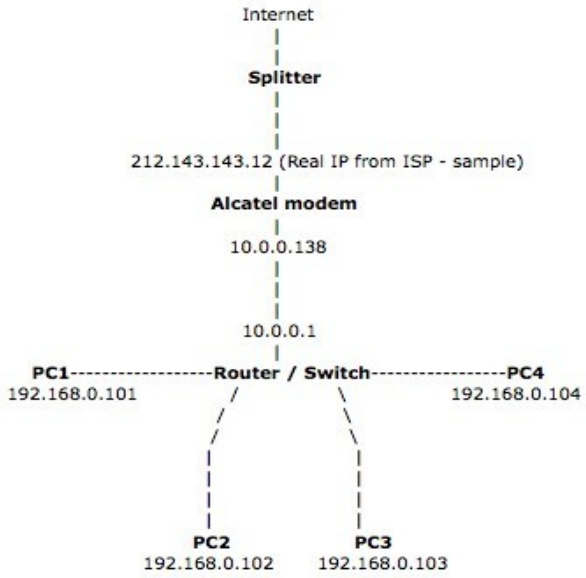


Figure 8. Network setup layout 4 (1) (with router or switch**)**

An ADSL cable goes to a splitter, the splitter is connects the ADSL modem. An Ethernet cable for the modem is connected to a router or a switch. After all PCs linked to the router or switch, configuration is needed to the router for Internet Sharing.

If an ADSL modem can function as a router between the Internet and the LAN, no router is required on the network in this case. Instead of the process to insert the Ethernet cable to a router or switch, a switching hub is the one that is needed to be

connected with. (Petri 2009). Figure 9 presents the second way of type 4 layout.

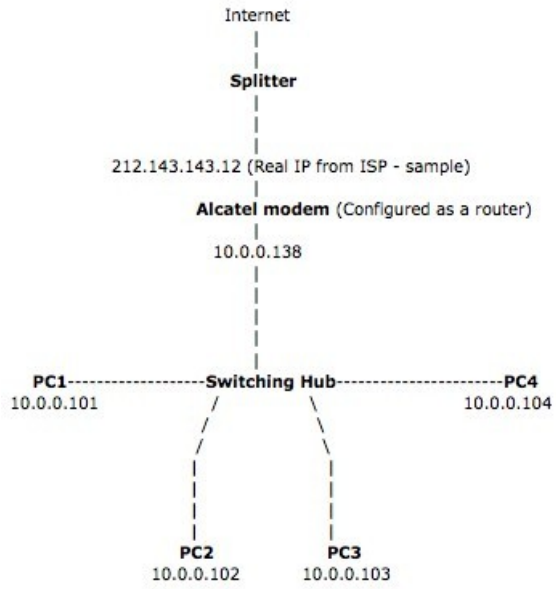


Figure 9. Network setup layout 4 (2) (ADSL modem with router function available)

If the ADSL Interconnection is not available in the residential environment at present, there are also other network layouts under the selection. These layouts are usable in all the Internet connections. The following layouts are summary based on the opinion of Bradley.

The first network layout is though a connection from a broadband modem to a wireless router. The devices included in this topology should possess a working network adapter, which have been introduced in Chapter 6. Technically, wireless routers allow dozen of PCs to connect over Wi-Fi links, while the network performance should be taken into consideration. Figure 10 below shows several network connectivity devices within the network: computers, printers and other entertainment devices. With a network interface card, other devices are also available to be inserted into the whole network environment. But the network range is the main limitation of using Wi-Fi technology. Without enough Ethernet connection existed, a network switch can be added to expand the wired portion of the layout. It can also be functioned as a pure wired network with the simply disable of wireless connection.

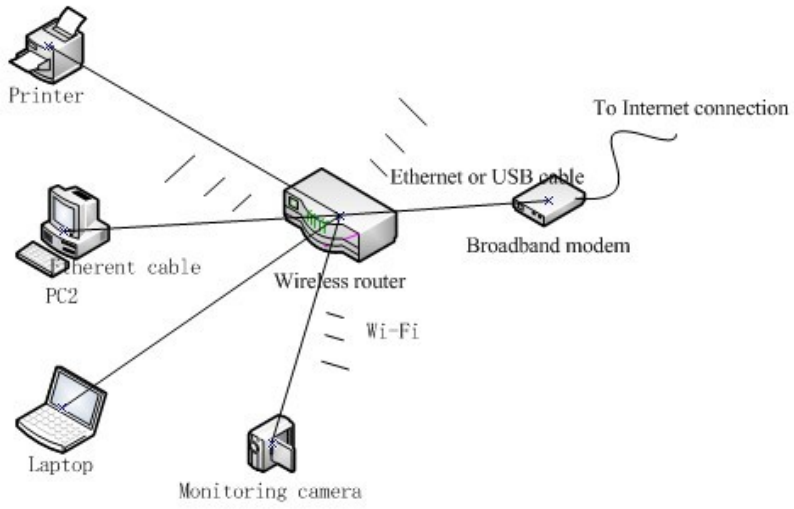


Figure 10. Network layout 1

The network connection can be also setup without a router presents by using Ethernet cabling. However, this network topology is not recommended for the home security system since only a single pair of computer or devices can be connected and additional devices can not join the network. In this circumstance, a whole control home security is hardly being built.

The second way to setup a home network is by using a hybrid network and wireless access point. Most (But not all) wired network routers allow up to four devices to be connected through Ethernet cable. Though a wireless access point consumes one port among four available ports, it enables dozens of Wi-Fi devices to join the network. But if all Wi-Fi available and PCs use the Internet at the same time, performance may slowdown. In addition, the wireless range is another shortage for the Wi-Fi portion of the network. Besides, all devices that connecting to an Ethernet router must possess a working Ethernet network adapter, and that connecting to a wireless access point must insert a working Wi-Fi adapter. A secondary device such as a network switch can be used to expand the wired portion of the layout if the wireless router does not support enough Ethernet connections.

The second network layout is illustrated below in Figure 11. It is possible to add more devices into the network only if the Ethernet network adapter is possessed.

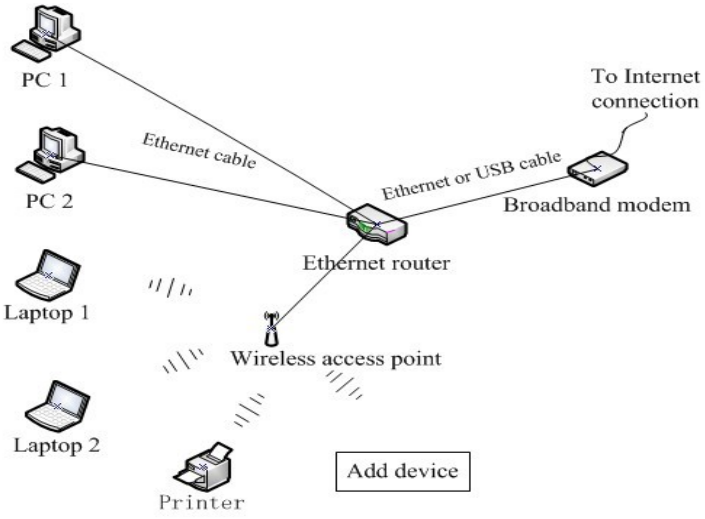


Figure 11. Network layout 2

The third option, in Figure 12, is so-called ad hoc wireless setup. An ad hoc wireless Wi-Fi eliminates the requirement of network router to access point in a wireless home network. With an ad hoc wireless function, network computers can be connected without reaching of one central location. Most people use ad hoc Wi-Fi only in temporary situations to avoid potential security issues. All the devices that connecting to ad hoc wireless must possess a working Wi-Fi network adapter with the "ad hoc" mode enable (Normally the mode is infrastructure). The typical limitation with a wireless network is security, although it is more flexible design compared to a wired network. The network bandwidth of ad hoc Wi-Fi network can be maximum as 11 Mbps, while other Wi-Fi networks may support 54 Mbps or higher.

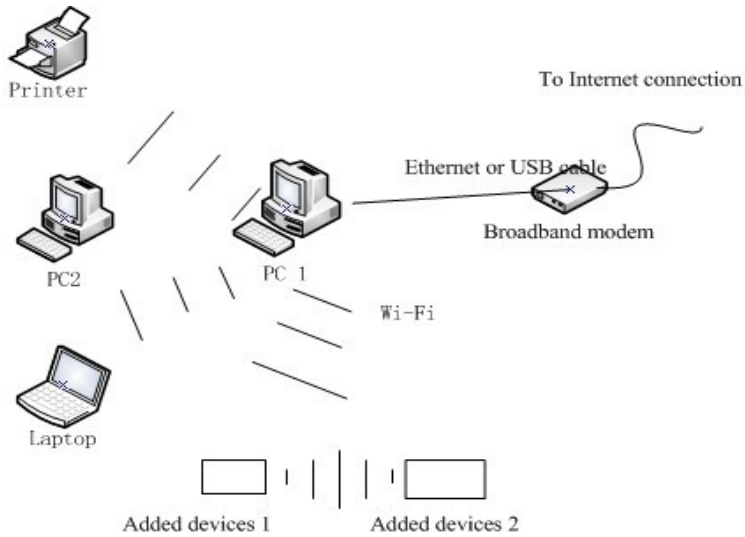


Figure 12. Network layout 3

The fourth option is to use an Ethernet hub or switch on a home network with a working Ethernet network adapter possess in all the connecting devices. The topology allows multiple wired computers to network with each other. Instead of setting up an interconnection directly through a hub or a switch, one computer must be designated to control the Internet connection. However, the wireless function is not including in this layout, so it is not practical for the home security system to function. Figure 13 covers this network layout.

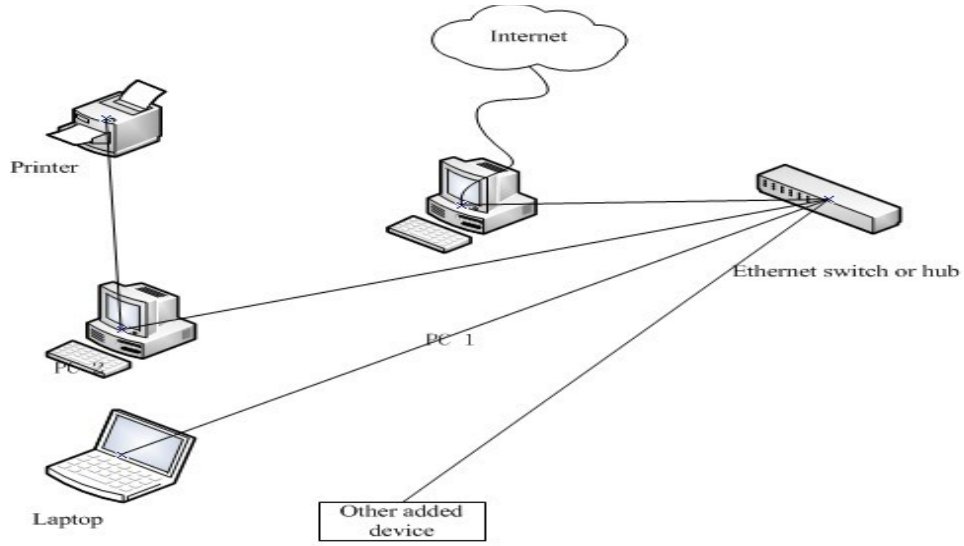


Figure 13. Network layout 4

The methods of network connectivity mentioned above are considered as a reference for home user to install the home network devices, and combined with the real situation of the home users such as the network connection media type, network device interfaces, and network speed, etc…

After setting up the basic home network, home security devices can be inserted to the whole home system based on the option of home users. For the basic level networking, a backup device, a webcam, and several of alarm devices are needed.

A backup device is usually connected to a PC. According to Arnief (2009), the Types of drive of a backup device are divided into USB, Network attached storage or “NAS” unit. An USB type plugs directly into a computer and install via a set of built in drivers. This type of device is generally only for backup the computer it is attached to. While a network attached storage device is attached through an Ethernet cable and allow all of

the computers that are attached to the network to share the device. The setup is achieved by connecting a supplied Ethernet cable to the broadband router, and installs the included setup CD on a computer to configure it. These two types of backup device are only kept a single copy the data, while with a "RAID" configuration, the data can be restored in a more secure way. RAID, Redundant Array of Inexpensive Disk, allows multiple disks to share in the duty of storing data. So a RAID including 2 hard drives makes a mirror of all data on both, can still ensure the safe of data if one drive fails. (Arnief 2009).

To install a webcam, a running PC, and a webcam utility are required. One Webcam utility is Dorgem, a free open source webcam utility which supports Operating System for Windows (Dorgem Web Capturer 2003). First, a home user needs to download the driver if it is not installed. Usually, the most common webcam vendors are Creative Labs, Logitech, Labtec, and D-Link. Then a home user should download and install Dorgem followed with the instructions present on screen. After installed Dorgem, a home user will see the camera selection list shown in Figure 14. Finally by clicking the preview button and adjusting the camera settings of webcam, Dorgem is successfully launched. From the source button, a home user can easily regulate the brightness, contrast and other settings. A notice to the Labtec webcam user is that this type of webcam may need to reconnect after a certain period of time if no motion is detected. A selection of use motion detection in General tab can restrict this action. But the user should try to keep the intervals at least in five minutes since the webcam may take picture every time when Dorgem reconnects to it that may lead to a failure capture of an actual motion. (Dorgem Web Capturer 2003).

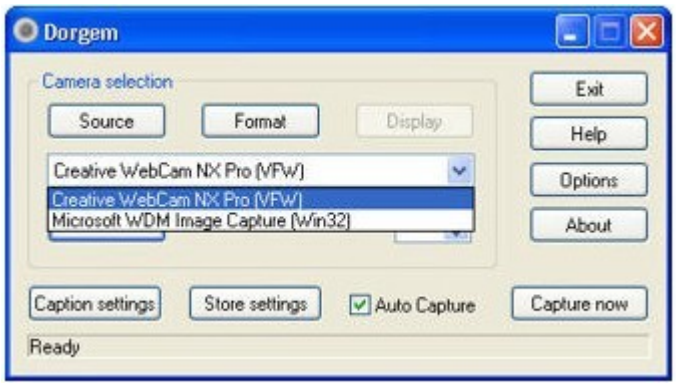


Figure 14. Camera selection of webcam

The advanced level of home security system contains Radio-frequency

identification （ RFID ） tags, Barracuda security card, and other advanced security function devices. All of them can be optional depended on the advanced security needs of the home users.

A backup capsule belongs to the advanced level of the home security system. It is used to store the backup images in a special secure place in the computer's hard disk. To avoid accidental deletion or unauthorized access to the disk backup images, the backup capsule is a hidden partition and thus cannot be mounted in the operating system. A single hard disk may contain only one backup capsule. However, the user can attach another hard disk with an existing backup capsule to the computer and restore from that as well without any problems. (Paragon Software Group 2011).

An Apple Time Capsule is one backup capsule device. There are several features of the Apple Time Capsule, such as automatic backup, simultaneous dual-band 802.11n Wi-Fi base station. The most important feature is the Apple Time Capsule works with Mac and PC as a wireless hard drive. (Apple 2009) Picture 15 shows the outlook of an Apple Time Capsule.

Picture 15. Apple Time Capsule

The setup process of an Apple Time Capsule can be divided into 3 parts. The first step is using Time Capsule with Time Machine. Time Machine detects Time Capsule on the network. Then user should create a wireless network. At last, it is possible to connect a printer to the USB port on Time Capsule in the wireless network. (Apple 2009) The detailed setup information can be found in Apple‘s official website.

7.3 SWOT analysis of home security system

SWOT analysis is a vital part during a scanning of the internal and external

environments during the strategic planning process. SWOT stands for strengths, weaknesses, opportunities and threats. There are two main categories that identify the internal and external factors. The internal factors can be classified as strengths and weaknesses. Opportunities and threats embody to the external factors.

The Strengths, considered the design of the home security system, were chiefly concluded in the following 4 points:

- Dividing user requirements into 2 levels;
- Flexible in use;
- Connecting different security subsystems into an integrated security system;
- Providing a secure way for residential environment.

The two levels design, basic and advanced, enabled to make alternatives for home users to choose the best option that fulfills their requirements. Instead of fragile subsystems, an integrated security system could apply more convenience to control residential environment.

Weaknesses are related to the practical part. This thesis was designed and developed based on the analysis of the theoretical works. Since there were not hardware devices available, the practical tests were impossible to do. However, this work is innovative in that sense that I constructed an integrated home security system that do not exists at the moment

The first angle of opportunities is that the residential environment needs a more reliable home security control system because of the living environment is becoming worse. Furthermore, as a result of an innovative technology (no computer based home security system exists at least in Finland and Sweden analysis from the Interviews); there will be more business opportunities in the market.

Considered the threats, compatibility was the fundamental factor before connecting devices. As mentioned in Chapter 4, the computer or network based home security system is innovative, so it requires time for people to take in. The people, who deliberate their home security system, mainly are focused on the basic function, such as door lock or smoke sensor. While the advanced function, Barracuda Card, for instance, demands more time for them to digest.

8 INFRASTRUCTURE PLAN FOR HOME SECURITY SYSTEM

Chapter 8 concludes an ideal model of a home security system that may not be viable and practical at present, but it could be a future design or tendency towards the development of home security systems and devices. A wireless network is an essential part of this thesis. If a wireless function enabled, wireless network interface card or network adapters have to be possessed to the devices in order to make the network functions. The infrastructure plan for home security system is mainly aimed to centralize the security devices so that the system is easy to set up and simple to control by a home user. The infrastructure plan operates also with a wired network.

From the interview and the discussion with my supervisor, Juha Meirläinen, the basic sensors such as smoking sensor, motion detection sensor in today's market usually do not have a wireless function available. They are merely working individually linger over the integrated system. Moreover, a central control is more than feasible to operate. So sensors are the preliminary devices to be inserted in the network adapter. The other optional devices such as game console, light controller, temperature controller are also require a network adapter if connecting to the home security system.

Figure 15 illustrate a physical topology of a home security system. The physical topology presents the devices on a network and how they communicate with each other.

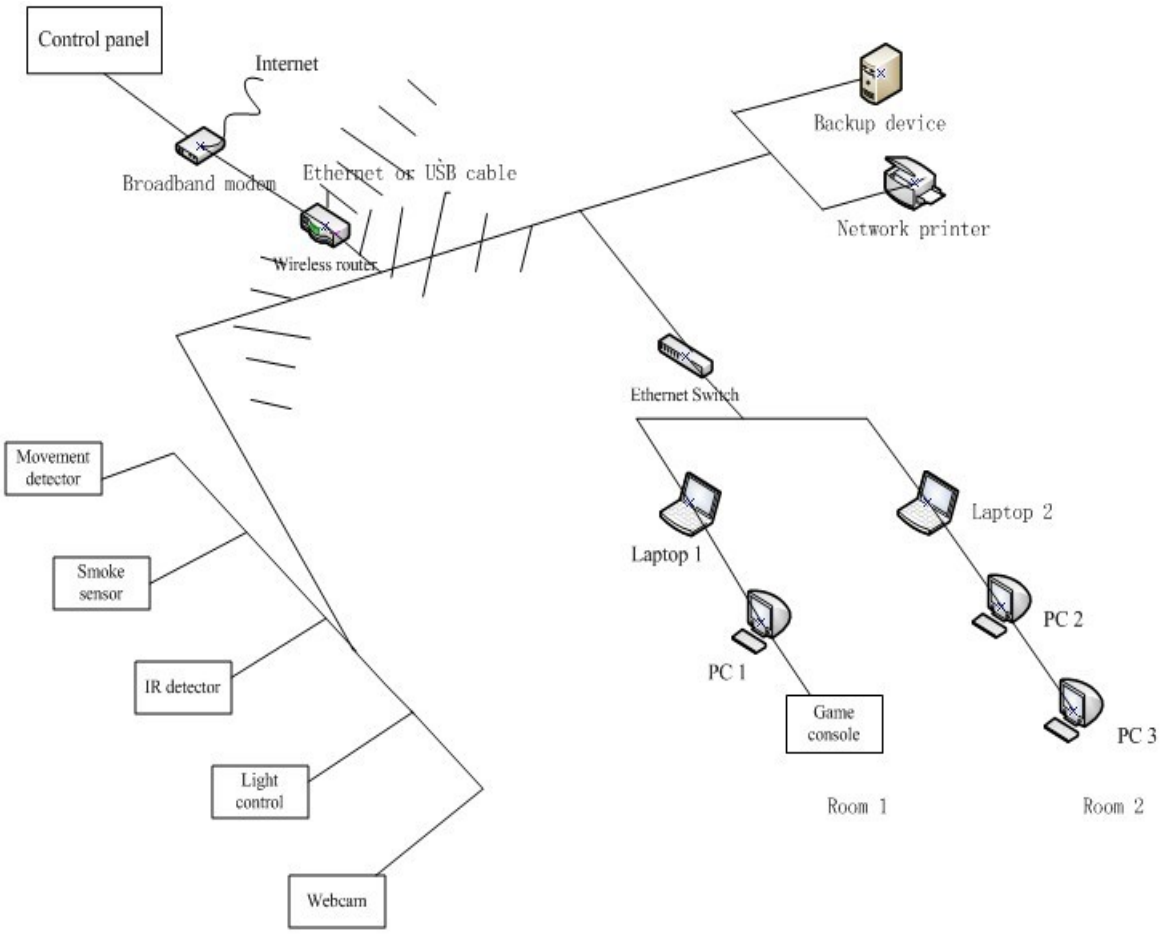


Figure 15. Physical topology of a home security system

In Figure 16, a logical topology of a home security system is presents. The logical topology shows the signal act on the network media, instead of a physical interconnection of the devices in a physical topology.

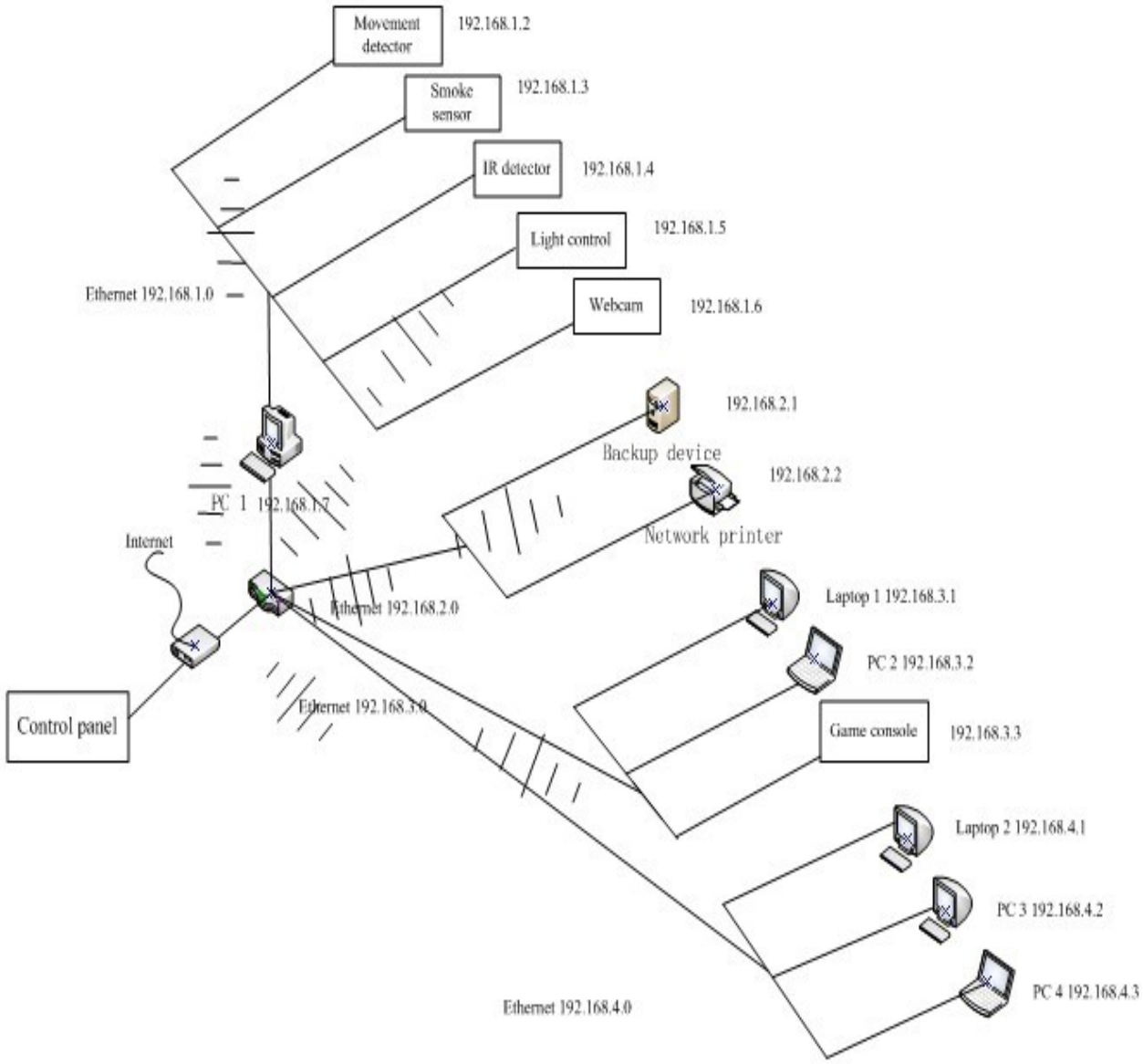


Figure 16. Logical topology of a home security system

Figures 15 & 16 are present both a physical and a logical topology of a home security system. A Control panel acts as an administrator of the whole security system. It is linked to a broadband modem. A router that is connected to the modem has been chosen to divide the network to domains. Because the home users need to insert the devices according to their own requirements, a switch is an optional option and so are also the added sensors. Wireless connection enables function of each network devices. A mix of a wired and wireless network connection is possible in the home security system. In Figure 16, four network domains are being built: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0. The other network domains are able to construct as the network topologies, Figures 15 & 16 are merely specified as an example. A computer is located between the control panel and sensors so that it could process the signal and store the data in its drive before the data transmit back to the control panel. Specific Software is installed in

the computer to identify fake alarms, with which, if emergency occurs, the warning message will be filtered, and the real warning message will be finally received by the control panel.

All the devices in the home security system must possess a network adapter so that it could be integrated to the whole system and under the central control of the control panel. The advised network adapter for each interface is wireless network card with a result that a central control is reached. A suggestion for desktops network interface is using network expansion card NICs based on the data analysis from Chapter 6. The reason is that they are typically designed for installation in a PCI (Peripheral Components Interconnect) slot on a computer's motherboard. PC Card network adapters are recommended to Portable PCs, such as notebook and laptop computers. The other types of network interface cards are not proposed such as a USB (Universal Serial Bus) network interface because it is not as popular as the former two network adapter mentioned above. Hot-installed is not necessary for home user despite it is one preliminary advantage of a USB network interface.

Although one network domain can operate well, dependence of the operation of the different network domains ensure the efficiency, the effectiveness and the security of the network. A network domain is also able to prevent network collision for the whole system. A switch can be applied to decrease the number of collision domains if there is a large network scale. It is because each port on a switch is it own collision domain. Nonetheless, if the home users only have a few network devices within the home security system, one network domain is enough for them to use.

The control panel is function as a real-time monitor; it records each activity that occurs within 24 hours. Home user can setup the deleting time of record history, or receive a warning message of the record history by the control panel when the cache is over the setting amount. If an emergency occurs, message will be send to both the home user and the service provider through the Internet and text message of mobile phone, which helps to prevent the situation if the network is crashed down.

In case there is an unstable voyage or power interruption of the power supply, a UPS (Uninterruptible Power Supply) is adopted into the home security system. A UPS is a device or a system that provides quality and continuity of an AC power source (Hickey

2003). UPS commonly includes equipment, backup power source(s), environmental equipment (enclosure, heating and ventilating equipment), switchgear, and controls, which, together, provide a reliable, continuous-quality electric power system. As the solution applied above, all of the home devices are required to connect with a UPS device except for the laptop with a battery inside. Although a UPS device has several jacks to link to the devices, location of the devices should be taking into account as cable might beyond its range. More than one UPS devices could be inserted into the whole system so that each important device can own its backup power supply.

Depended on the requirements of the home users, they can choose the devices either in the basic level or the advanced level. In the solution of Chapter 8, only the basic level devices have been listed due to the basic level is suitable for most of the home user. These devices are Router, switch, broadband modem, smoke sensor, movement detector, IR detector, light control and web camera.

9 CONCLUSION

Home security system may be considered to enlarge its scalability and included more functionality in 5 more 10 years (Interview 2011). However, the major functions and requirements are not expected to differ significantly, while security, simplicity and affordability will be on the top priority. Future services may contain user friendliness requirements, low installation costs and device expenses requirements, quality of services requirements and interoperability requirements.

The user friendliness requirement is mainly for a customer with little computer experience. Thus the technologies and the applications should be operating as simple as possible, and be easy to install. The features such as auto configuration and remote maintenance can be integrated to the system as well. As time goes by, a large market share of home security system will incur the lower expenses of security devices and the installation costs. Quality of service requirements should be applied by the service provider to guarantee limited delay, minimum jitter and other limitation that exists in the home security system. Since there are types of devices and products from various companies coexist in one home, the interoperability assists to define a universal standard for the associations. The associations may be formed by several service providers.

One specific solution of a home security system have been produced in this thesis, home user can use it as a reference when construct their own home security system. Although the infrastructure plan for the home security system only remains on the theoretical stage, it can be implemented in future when the technology of devices is mature. Along with the reality that the safety of life is decreasing, home security is increasing its pace for a home user to take actions.

REFERENCES

Printed

Glister, Ron 2002. PC Hardware: A beginner's guide. McGraw-Hill Professional Publishing, USA.

Gilster, Ron & Heneveld, Helen 2004. HTI + Home Technology Integration and CEDIA Install I All-in-one Exam Guide. McGraw-Hill Professional Publishing, USA.

Hair Joseph & Money Arthur, Page Mike & Samouel Phillip 2007. Research Methods for Business. John Wiley & Sons. Chichester.

Hickey, Robert B 2003. Electrical Engineer's Portable Handbook. McGraw-Hill Professional Publishing, USA.

Lindstrom, Pete & Thornton, Frank 2005. RFID Security. Syngress Publishing, Canada.

Long, Larry 2002. Home Networking Demystified. McGraw-Hill Professional Publishing, USA.

Lopez, J & Zhou, J 2008. Wireless Sensor Network Security. IOS Press, Amsterdam.

Ross, John 2009. Network Know-How: An Essential Guide for the Accident Admin. No Starch Press, San Francisco, USA.

Purser, Steve 2004. A Practical Guide to Managing Information Security. Artech House Incorporated, USA.

Coleman, Pat & Nelson, Stephen L 2000. Effective Executive's Guide to the Internet: The Seven Core Skills Required to Turn the Internet into a Business Power Tool. Consortium of Collective Consciousness, USA.

Not printed

Apple 2009. Time capsule setup Guide. Downloaded May 2010. <http://manuals.info.apple.com/en/TimeCapsule_SetupGuide.pdf>

Arnief 2009. How to Select a Home Backup Storage Device. Downloaded December 2010. <http://www.ehow.com/how_5111431_select-home-backup-storage-device.html>

Bruin Online 2009. Virtual Private Networking (VPN) using PPTP. Downloaded November 2010. <http://www.bol.ucla.edu/services/vpn/pptp/>

Dorgem Web Capturer 2003. Updated in January 2003. Downloaded January 2011. <http://dorgem.sourceforge.net/>

Lukko Oy & Gränslås 2010. An Interview in Tornio & Sweden. 9th October 2010.

Meriläinen, Juha 2010. Discussion with the supervisor. 19th May 2010.

Mitchell, Bradley. Gallery of Home Network Diagrams. Downloaded November 2010. <http://compnetworking.about.com/od/homenetworking/ig/Home-Network-Diagrams/index_t.htm>

Paragon Software Group 2011. Updated in 2011. Downloaded January 2011. < http://www.paragon-software.com/home/systembackup/>

Petri Daniel 2009. Home Network Setup – What are the possible configuration settings for a home/SOHO network with 3-4 computers and an ADSL Interconnection. Downloaded November 2010. <http://www.petri.co.il/adsl_home_network_config.htm>

R. Kayne 2010. What is ADSL? Downloaded November 2010. <http://www.wisegeek.com/what-is-adsl.htm>

Shostack, Adam & Stone, Adrian & Penta, Anthony & Neerumalla, Bala & Dang, Bruce & Seifert, Christian & Canavor, Darren & Stathakopoulos, George & O'Dea , Hamish & Jones, Jeff & Faulhaber, Joe & Lambert, John & Ness, Jonathan & Pottorff, Paul & Boscovich, Richard & Wu, Scott & Mordani, Ritesh & Parthasarathy, Sasi & Reasor Sterling & Zink, Terry & Lee, Tone & Campana, T J & Gullotto, Vinny & Huang, Yuhui & Mador, Ziv 2009. Microsoft Security Intelligence Report volume 7 June 2009. Microsoft download center. Downloaded May 2010.

<http://download.microsoft.com/download/A/3/0/A30A60D9-1303-4B6A-91B7-BB24E0211B05/Microsoft_Security_Intelligence_Report_volume_7_Jan-Jun2009.pdf>

Taylor, Dena 2009. The Literature Review: A Few Tips On Conducting It. Downloaded December 2010. <http://www.writing.utoronto.ca/advice/specific-types-of-writing/literature-review>

TechTarget 1999. SearchNetworking.com Definitions. Download November 2010. <http://www.backtrack.org/barracuda/barracud.pdf>

West Coast Publishing 1999. The Barracuda Anti Theft Device. SC INFO Security Magazine. Downloaded May 2010. <http://www.backtrack.org/barracuda/barracud.pdf>

Appendix 1

QUESTIONNAIRE FOR HOME SECURITY SYSTEM

The questionnaire, designed for a thesis, is about an infrastructure plan for home security system that combines different home security devices into one integrated system in order to achieve the home security goals.

Basically, the home security system is include

- Wired / wireless network
- Backup device, e.g. Apple Time Capsule
- Web-Camera monitoring system (movement detector)
- Electric locks
- Alarms (mobile phone, e-mail) warnings
- Other security devices.

The advanced devices are as follows:

- Radio-frequency identification（RFID）tags
- Barracuda security card.

RFID tags are used for tracking all the vital equipment within in the home range and all the information will be recorded in the home computer. Barracuda security card, or the CUDA Card, which is installed in computer, can be used to protect your computer from theft and tampering by using an ambient light sensor. The CUDA Card is shown in Picture 1.

Picture 1. Barracuda security card

Notes: the basic level is for the basal protection of home security. The advance level means the security zone(s) that home user designed contains sensitive data that should be more focused on.

Besides, user can make their own option depend on what their needs, saying, there is no need to include all the devices that list above to your home security system.

✓ Use this symbol to copy and paste to the square if you using the electronic edition.

1. Quantity or information

Age: under 30 ☐ 30-50 ☐ over 50 ☐

Do you have demand to install or improve your home security system?

Yes ☐ No ☐

If yes, which security level:

basic ☐ advanced ☐

2. Ranking

Choose a suitable level for your existing home security system:

very high ☐ high ☐ middle ☐ low ☐ very low ☐ none ☐

3. Single selection

How much do you ready to pay for your home security system? (Unit: euro)

500-1000 ☐ 1000-1500 ☐ 1500-2000 ☐ 2000-2500 ☐

How fast should the help come to your home?

within 5 minutes ☐ within 10 minutes ☐ within 15 minutes ☐

within 20 minutes ☐ More than 30 minutes ☐

How long time do you want the system to archive information, such as video?

within 10 seconds ☐ within 30 seconds ☐ within 1 minutes ☐ within 2 minutes ☐

other _____

How long delay between going in and turning off the security system?

within 10 seconds ☐ within 30 seconds ☐ within 1 minutes ☐ within 2 minutes ☐

other _____

4. Multiple choices

What devices do you want to connect to your home security system?

- ☐ · Wireless router
- ☐ · Backup device
- ☐ · Web-Camera (movement detector)
- ☐ · Electric locks
- ☐ · Alarms, sirens, sounders
- ☐ · Sensors (motion sensor, smoke detector…)
- ☐ · Radio-frequency identification（RFID）tags
- ☐ · Barracuda security card
- ☐ · External security services (focus on outside home remote monitoring, such as alarm monitoring, remote viewing monitoring)

5. Open-ended

What the system should do when detecting an alarm?

(Please make them into order):_____

1) Send an alarm message to my cell phone
2) Send an alarm to the security company
3) Lock all the doors and locks
4) Warn about event
5) Silent alarm and make record
6) Other:_____

Do you usually have problems to connect security devices to the system? If so, what is the most difficult part for you?

_____

_____

_____

Where do you want the system to store information? Such as home, Security Company,

external service providers such as Google...

In which way that you want the user interface work? Such as plastic card, keyboard, biometric detection, voice...