Explore Security Threats in Computer Laboratory Systems

Bambarandage H[1]
Perera GAKS[2]

ABSTRACT

Computer systems are vulnerable to many threats that can inflict various types of damages resulting in significant losses. Threats are Errors and Omissions, Fraud and Theft, Employee Sabotage, Loss of Physical and Infrastructure Support, Malicious Hackers, Industrial Espionage and Malicious Code. The damage can range from errors harming database integrity to fires destroying entire computer centers. Precision in estimating computer security-related losses is not possible because many losses are never discovered and others avoid unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.

Threats can be divided into two parts as Software threats and Hardware threats. Software threats can be easily disturbed by using Antivirus or Internet Security Software. Hardware threats can be eliminated by using modern access controller time attendance machine. But the problem is that it is very expensive.

In this study, it was attempted to design a low cost system to eliminate hardware threats. A card and a machine were produced locally at low cost. Card uses resistor method for identifying the users correctly. The machine converts analog signal to digital signal and encrypted data are passed to the computer. Also Software was generated locally to store user information. Server computer is handled by the user. Server can prohibit some users. The new design product can be used in universities, schools, etc.

KEYWORDS: Software, Hardware, Threats, Security, Computer

INTRODUCTION

A computer laboratory, also known as a computer suite is typically a room which contains many networked computers for public use. Computer laboratories can be found in libraries, schools, government buildings, science laboratories, community centers, companies with IT departments that require such a place for their employees to do their jobs and research centers. They are distinct from internet cafes.

Printers, scanners and other peripherals may be augmenting the laboratory setup.

All computer users (staff, students, and others) are expected to be responsible for their own behavior on the computer system, including the internet just as they are anywhere else. Users are reminded that their actions can represent the entire community.

Though many regulations are implemented, threats occur in computer laboratories at a rapid rate.

It has been noticed that one reason for this is due to the use of computer laboratories by unauthorized personal. So, in this study attention has been paid to stop such person's entrance to computer laboratories. For that a system was designed consisting of a card, machine operated with a software linked to the main server.

[1]Graduate, Department of Electronics, Faculty of Applied Sciences, Wayamba University of Sri Lanka.

[2]Senior Lecturer, Department of Electronics, Faculty of Applied Sciences, Wayamba University of Sri Lanka

LITERATURE REVIEW AND THEORETICAL BACKGROUND

Computer systems are vulnerable to many threats that can inflict various types of damages resulting in significant losses. These damages can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are avoided unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.

Basically security threats in a computer laboratory can be divided into two parts.

1. Software threats
2. Hardware threats

Normally, viruses, worms, trojan horses, logic bombs, and other "uninvited" software are software threats in computer laboratory. These threats can be eliminated by using antivirus/internet security software. Also these softwares must be updated. Antivirus /internet security software can be obtained at a low cost.

In computer laboratory systems, basic hardware threats are fraud and theft, unauthorized access. For avoiding these threats, simple solution is to have a security person. But the problem is how to identify the unauthorized persons. There exist some products for avoiding these things. But these products are at high cost. (Harris, Shon, 2005)

RESEARCH APPROACH AND METHODOLOGY

Data was collected from a company and people who are in IT field. Questionnaire was given to people who are in company and Sri Lanka telecom. Minor interviews were carried out with few selected individuals from the hardware department and software department as to get brief discussion about security threats, software and hardware solutions.

Questionnaires were distributed among the employees to determine how they have acted at the beginning of their career at company. The questionnaires included two parts, sixteen multiple choice questions and one structural question. The contents of the questionnaires were prepared based on interview and discussion. Probability of responses was calculated.

DATA COLLECTION AND ANALYSIS

Responses for the questionnaires conducted with the hardware department software department and out siders who are in IT field.

Table 1. Details of Data Analysis (Probability)

Description	O/L	A/L	Degree
Software Knowledge	0.89	0.94	0.96
Software Price satisfaction	0.78	0.88	0.94
Software Product satisfaction	0.78	0.78	0.90
Hardware Knowledge	0.56	0.91	0.92
Hardware Price satisfaction	0.56	0.84	0.88
Hardware Product satisfaction	0.22	0.25	0.14

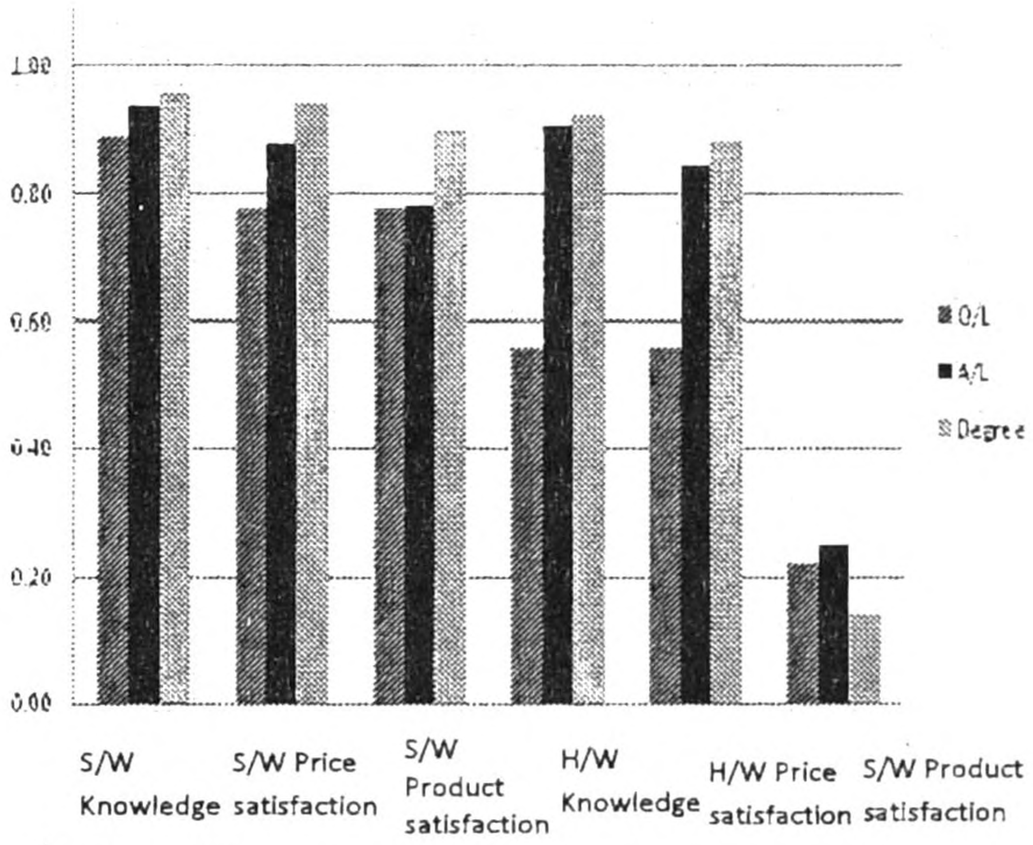

Fig 1. Graph of data analysis

According to the above figure, in the O/L category software knowledge is about 0.89. In the A/L category knowledge is higher than O/L category. And knowledge is highest for those holding a degree. O/L category software price satisfaction is about 0.78 and it is about 0.88 in A/L category. In degree category software price satisfaction is highest. O/L category and A/L category have nearly same in software product satisfaction. And degree category software product satisfaction is highest. Hardware knowledge of O/L category is lesser than A/L and degree category. O/L category hardware price satisfaction is about 0.56. The A/L category hardware price satisfaction is about 0.84. And degree category hardware price satisfaction is highest. O/L category hardware product satisfaction is about 0.22. The A/L category hardware product satisfaction is little bit higher than O/L category. And degree category hardware product satisfaction is the least from all.

By considering those data, it is seen that all three categories have good knowledge of software threats and software solutions. That means they have a clear idea about what are the existing products and how to use them. All three categories have good software price satisfaction. It means they can get the software solutions with a satisfactory value. Products satisfaction of the software is high. So that, software products and its prices are good enough to protect from the software threats. Hardware knowledge of the people, who educated till the O/L, is lower than others. That means people educated more have the knowledge about hardware threats and hardware solutions. All three categories have average knowledge and price satisfaction of the hardware. That means all three categories think existing products have a lot of functions. Therefore they think that is reasonable price. Computer laboratory systems are using access control only. It is a waste money because of high cost limited outcome compared to the investment. With the above data, it can be concluded that all categories have low hardware product satisfaction.

IDENTIFICATION OF CAUSES AND SOLUTIONS

People have good knowledge of software threats and software solutions. And they have a reasonable idea about price of existing software products. Also they think existing products can be used in local computer laboratory system. All three categories have good average knowledge about hardware. People think existing products have lot of functions. Therefore they think that is reasonable. Because of that hardware price satisfaction is high. But all three categories think existing hardware products can't be used in local computer laboratory system.

Existing hardware products have lot of functions. But local computer laboratory systems use only access controller part. But whole product should be purchased. Therefore unnecessary cost is spent. So as a solution the machine which has only the access controller part can be produced locally at low cost.

The price of the product must be low and the machine should control the access doors. And product operation, maintenance and service should be able to do easily with low cost.

New design has the capability of access controlling. That means machine is able to select authorized person and open the door. It is the important point of the system. Also it can be produced at a low cost. All users have an access controller card. This card may be the identity card of the user. User must use this card to enter the computer laboratory.

This card can be produced locally at low cost. Considering the machine, it can be used easily and every one can understand how to enter the laboratory.

DESIGNING OF THE SETUP

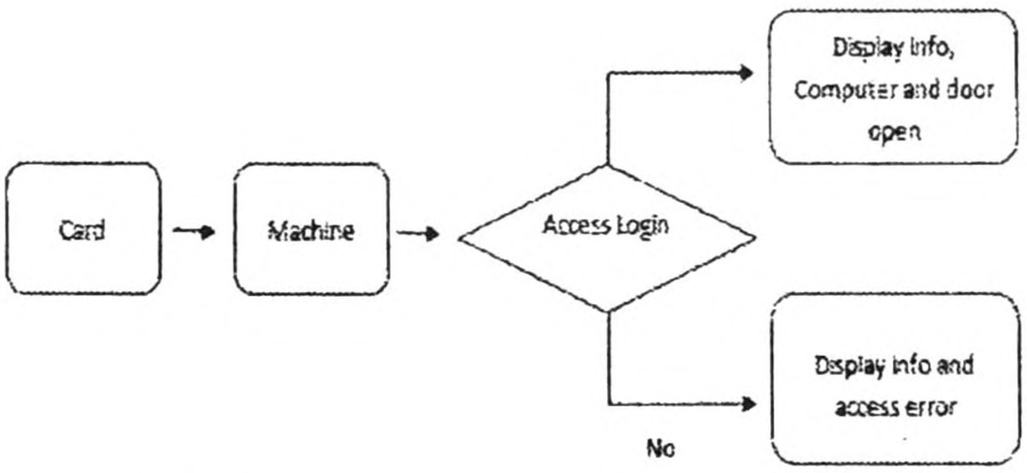

Fig 2. Block diagram of the product design

1) Access Control Card

Access Control Card is a plastic card used to gain/control access to enter computer laboratory. Usually it is associated with magnetic or chip cards and proximity cards with or without photo e.g. ID badges. In this system, it uses R card. That means this card uses resistance to change the users. Different cards have different resistance values.

2) Access controller machine

When the card is used, value is passed to the machine. The machine receives an analog signal. It is converted into a digital signal. The machine accepts the card number of the user.

Numerical number is sent to the computer connected to the server computer. It has all information about the user.

Server computer send the data base to computer which is connected with machine. The computer displays all the information about the user.

Further server checks whether there are any available computers in laboratory. Then the server will send the computer number. If the card is a valid one then the door will open.

3) Final Product

Serial connection is used for connecting access controller machine with the computer. Data is passing to the computer by using RS 232 protocol.

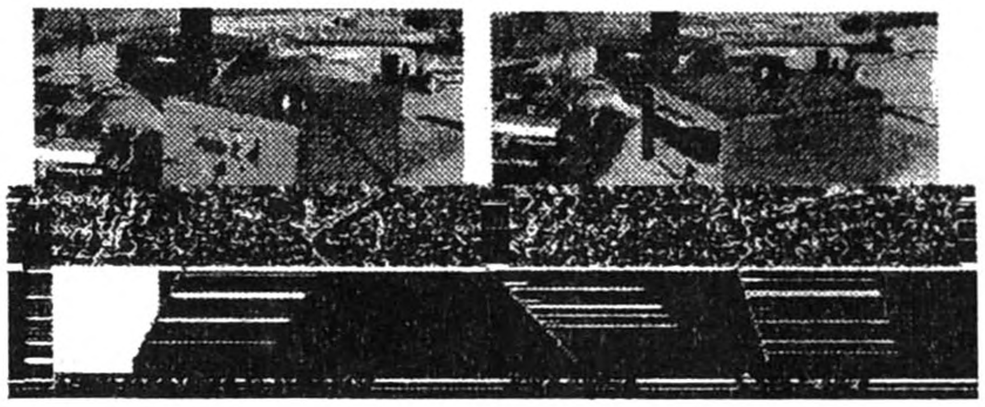

Fig 3. Outlook of the final product

Push Button is used for resetting the machine. When the card is inserted in to the card reader, it reads the card.

4) Software Design

Fig 4. Normal window in access controller system

This is a normal display. That means no user is using access controller system. System time and Date is shown on computer display. News tag is used for showing the latest news. It is controlled by the server (/Administrator.).

When someone is using access controller system, the display will show in the following interface.

Fig 5. User login

Fig (5) shows the student ID (that means registration number in university.),

student name, card number (Shown in the card), faculty and computer number (selected by the server computer.)

DISCUSSION AND CONCLUSION

Limitation of the Research

Physical access controls are one way to prevent/ identity fraud. However, in a security environment, it is the best practice to combine physical access controls with logical authentication types. In order to provide a higher level of security, it is more effective to authenticate users based on a mix of logical authentication types. Below are three types of authentication.

- The first type of authentication, which pertains to passwords, personal identification numbers (PIN), and information that only the individual should know.
- A second type of authentication is a key or a smart card.
- The third type of authentication that cannot be misplaced or forgotten is referred to as a biometric. Biometric information is part of a person.

This system uses,

- R Card.
- Access control machine
- Access controller Software

Problems

- Other persons' R card can be used for accessing the laboratory

R card can be used by anyone because it hasn't biometric information.

- User must wait until a computer is selected by the server

After inserting the card, all the information are displayed on the screen. But the user is unable to select a computer. The server checks whether there are any available computers in the computer laboratory. After that, server will send the computer number to the user. Then only the door will open.

- User can't choose computer

As the server issues the number, the user can't select a computer.

Further Development

According to the International Biometric Group, biometrics uses automated physiological or behavioral characteristics to determine or verify identity and physiological biometrics are based on measurements and data derived from direct measurement of a part of the human body.

Fingerprints constitute one of the most important categories of physical evidence and it is among the few that can be truly individualized (Lee and Gaensslen 2001). A fingerprint recognition system is commonly used for identification purpose. They are only designed to capture and distinguish the unique impressions of distinct ridges on the fingertips and valleys.

There are two types of fingerprints: flat or rolled. Flat prints are an impression of only the central area of the finger pad while rolled prints capture ridges on the sides of the finger as well as the central portion between the tip and first knuckle. (Rosenzweig, Kochems, and Schwartz 2004). Fingerprint images are scanned, enhanced and then converted into templates. These templates are saved in a database for future comparisons using scanners such as optical, silicon or ultrasound. Even though ultrasound appears to be the most accurate, they are rarely used. Optical scanners are the most commonly used.

Some people are uncomfortable with this technology because they feel taking a fingerprint is similar to identify as a criminal and tend to resist its use as a biometric. Another concern is that fingerprints collected for one purpose could be used to track an individual's activities. In addition, fingerprint biometric systems do not work everywhere, for example, in gloved environments like operation theaters in

hospitals. One area where fingerprint biometrics has been used for identity and access management in health care. The biometric technology is a solution to how hospitals can give access to users and yet maintain security levels that provide confidence and comfort. This is a critical challenge since greater security usually decreases access. There have been very few complaints about the technology in hospitals. People seem comfortable with having their fingerprints stored in a database since it was stored as a string of numbers rather than the actual digital image.

DISCUSSION

By using this machine, unauthorized hardware access can be eliminated. This machine can be manufactured in the country for a low cost. By providing the optical finger scanners the accuracy can be increased and it can be marketed as a fully completed access controller machine.

REFERENCES

- Lee, Henry C. and Gaensslen R. E., (2001) Advances in Fingerprint Technology, CRC press

- Rosenzweig, Paul; Kochems, Alane; and Schwartz, Ari; (2004)"Biometric Technologies: Security, Legal, and Policy Implications," The Heritage Foundation, No. 12

- Harris, Shon (2005), *All-in-one CISSP Exam Guide*, Third Edition, McGraw Hill Osborne, Emeryville, California