UNIVERSITI PUTRA MALAYSIA

# DEVELOPMENT OF SECURITY IDENTIFICATION AND MONITORING SYSTEM FOR WEB APPLICATION

NORIZAWATI DANI

# DEVELOPMENT OF SECURITY IDENTIFICATION AND MONITORING SYSTEM FOR WEB APPLICATION

NORIZAWATI DANI

MASTER OF SCIENCE
UNIVERSITI PUTRA MALAYSIA

1999

# DEVELOPMENT OF SECURITY IDENTIFICATION AND MONITORING SYSTEM FOR WEB APPLICATION

By

NORIZAWATI DANI

Thesis Submitted in Fulfillment of the Requirements for the
Degree of Master Science in the
Faculty of Engineering
Universiti Putra Malaysia

August 1999

# ACKNOWLEDGEMENTS

I would like to thank Prof. Dato' Mohd Zohadie Bardaie, Dr. Abd. Rahman and Prof. Madya Mohamed Daud for their continuous support, guidance and encouragement in completing this thesis. Thank you to PASCA Program and IRPA research program for the financial support and the research opportunity. To my ESEIA group especially Vicky, Foo and Aljack, thank you for the teamwork and assistance. I would also like to thank my family for their endless love, support and sacrifice. Thank you also to my special friends who are always beside me when I need them. Without all of you, this thesis would not have been written. Thank you very much.

## TABLE OF CONTENTS

# LIST OF TABLES

## LIST OF FIGURES

# LIST OF ABREVIATIONS

| | |
|---|---|
| SecureApp | Security Identification and Monitoring System for Web Application |
| PGP | Pretty Good Privacy |
| COPS | Computer Oracle and Password System |
| SATAN | Security Analysis Tools for Auditing Networks |
| DES | Data Encryption Standard |
| IDEA | International Data Encryption Algorithm |
| WWW | World Wide Web |
| SDLC | Software Development Life Cycle |
| ESEIA | Expert System for Environmental Impact Assesement |
| CLIPS | C language Intergrated Production System |

Abstract of thesis submitted to the Senate of Universiti Putra Malaysia in fulfillment of the requirements for the degree of Master Science

# DEVELOPMENT OF SECURITY IDENTIFICATION AND MONITORING SYSTEM FOR WEB APPLICATION

By

**NORIZAWATI DANI**

**August 1999**

**Chairman : Professor Madya Mohamed Daud, Ph.D.**

**Faculty : Engineering**

Security is an essential entity to any software application. The most famous threat to any software application is unauthorized updating and deleting of the application and data. Characteristics of a software application that could contribute to the degree of security concerns are accessibility, forgery, vulnerability and density. If the software application contains most of these characteristics, the more vulnerable it would be to any security threats. Thus, a web application being an open application and contains all of the characteristics faces the most degree of security concern and open to all possibility security threats such as hacker, eavesdropping and spooling. A security system that would secure the web application from most of the security threats is crucially needed.

The findings of this research is in the form of a prototype of a security system specifically for a web application. The web application that it secures is a knowledge application. The prototype is called SecureApp. It is developed by using Microsoft Visual Basic as its development tool and Microsoft Access as its database package. SecureApp consists of two main applications which are User Identification and Security Administration. These applications follow a predetermined security policy developed to protect the web application. Theory of encryption is used in its design and development for both applications especially to secure the passwords. SecureApp gives solution to the problem of securing a web application from any unauthorized users and other threats. The Security Administration application would allow the Security Administrator to monitor and detect any users who tries to breach the security policy of the web application. Whereas, the User Identification application would secure the web application and ensure that the security policy of the web application is not breached.

As a conclusion, security system for a web application is very crucial and its development could not be left out until the final stage of the implementation. The security system should be considered during the definition of user requirements and incorporated to the web application during the design stage. Thus, SecureApp would give solution in securing any web application. It would simplify and speed up security implementation without compromising the security policy needed by the web application.

Abstrak tesis yang dikemukakan kepada Senate Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains.

## PEMBINAAN SISTEM PENGENALAN DAN PENGAWASAN KESELAMATAN BAGI APLIKASI WEB

Oleh

**NORIZAWATI DANI**

**Ogos 1999**

**Pengerusi : Professor Madya Mohamed Daud, Ph.D.**

**Fakulti : Kejuruteraan**

Keselamatan adalah ciri yang penting bagi sebuah aplikasi komputer. Ancaman yang paling utama bagi aplikasi komputer ialah aktiviti membaiki and menghapus aplikasi dan data oleh sebarang pengguna tanpa kebenaran. Ciri-ciri aplikasi komputer yang boleh meningkatkan keprihatinan terhadap isu keselamatan ialah kemudahan diperolehi, pemalsuan, tahap kekebalan dan kepaduan data yang disimpan. Sekiranya aplikasi komputer mempunyai kebanyakan ciri-ciri tersebut, bertambah mudahlah ianya diserang oleh ancaman-ancaman dari pelbagai pihak. Memandangkan aplikasi web adalah sebuah aplikasi yang terbuka dan mempunyai kesemua ciri-ciri tersebut, ia menghadapi ancaman yang banyak seperti pengguna yang tidak diundang, pencuri maklumat melalui talian Internet dan pengguna misteri. Oleh itu sebuah sistem keselamatan yang khas untuk menghalang ancaman-ancaman ini dari menyerang aplikasi web adalah sangat-sangat dikehendaki.

Hasil dari penyelidikan ini ialah satu prototaip sistem keselamatan untuk aplikasi web. Aplikasi web yang dilindungi ialah sebuah aplikasi ilmu. Prototaip yang dibina diberi nama SecureApp. Perisian yang digunakan ialah Microsoft Visual Basic dan pakej pangkalan data yang dipilih ialah Microsoft Access. SecureApp mengandungi dua aplikasi yang utama iaitu Aplikasi Pengenalan Pengguna dan Aplikasi Pengawasan Keselamatan. Aplikasi-aplikasi tersebut bercirikan satu polisi keselamatan yang dibina khas untuk melindungi sebuah aplikasi web. Teori kod rahsia yang dikenali sebagai encryption digunapakai dalam merekabentuk sistem ini terutamanya untuk melindungi kata rahsia. SecureApp memberi penyelesaian kepada masalah bagaimana menghalang pengguna yang tidak diundang daripada menggunakan aplikasi web. Aplikasi Pengawasan Keselamatan membolehkan pihak pengurusan mengawasi pengguna bagi mengenalpasti sebarang kejadian melanggar polisi keselamatan aplikasi web tersebut. Aplikasi Pengenalan Pengguna melindungi aplikasi web dan memastikan agar polisi keselamatan dipatuhi.

Sebagai kesimpulannya, sistem keselamatan bagi aplikasi web adalah amat penting and ianya tidak seharusnya diberi perhatian hanya di peringkat akhir pembinaan aplikasi web tersebut. Sistem Keselamatan perlulah diambilkira semasa proses definasi keperluan pengguna dan diimplementasikan semasa proses pembinaan aplikasi. Akhir kata, SecureApp adalah penyelesaian kepada masalah keselamatan bagi aplikasi web. Ia membolehkan usaha implementasi keselamatan dapat dijalankan dengan cepat dan mudah tanpa menjejaskan polisi keselamatan aplikasi web.

# CHAPTER I

# INTRODUCTION

ISO 7498-2 security architecture defines security as minimising vulnerability of assets and resources. An asset is anything of value and vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security ( Pabrai and Gurbani, 1996). Examples of assets in computing technology are data, applications or software, hardware, network and communication. Each of these assets has its own vulnerability and threats.

Security threats can be classified as accidental, intentional, active and passive (Pabrai and Gubrani, 1996). Accidental threats exist with no predetermined intent. Intentional threats can be defined from casual examination of computer or network data to sophisticated attacks using system knowledge. Passive threats are those if happen do not bring any damage or modification to information in the system. Whereelse, active threats will bring damage and modification to the information contained in the system if occurred. (Pabrai and Gubrani, 1996)

Computer security is applied as connoting threat concepts and the physical and logical techniques applied in protecting the electronic computer and communication systems (Baskerville, 1988). It also includes concepts, techniques, and measures that are used to protect computing systems and the information they are maintaining against deliberate or accidental threats (Summers, 1984).

Security concerning each of the assets has its own definition. Information security is defined as the broader view, including systems analysis and design methods, manual information systems, managerial issues, and both societal and ethical problems (Baskerville, 1988). Data Security consists of procedures and actions designed to prevent the unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional, of the data (Madron, 1992).

With the growing popularity of network and communication in recent years, security moved to the same direction. Network security consists of those measures taken to protect a network from unauthorized access, accidental or intentional interference with normal operations, or destruction, including protection of physical facilities, software and personnel security (Madron, 1992). Where else, Communication Security (COMSEC) can be defined as protection resulting from the application of cryptosecurity, transmission security, and emission security measures to telecommunication and from the application of the physical security measures to communication security information (Madron, 1992)

In developing a security policy and system, identification of assets to protect is the most important criteria. It will define the design of security needed in protection the information confined in the computer system. For example, if an asset is defined as knowledge application that is shared through the internet, then the design of the security system would concentrate on how to protect the application , the knowledge rules and knowledge database from unauthorized users and other threats.

A knowledge application can also be defined as an expert system. Expert systems are computer programs designed to help in solving problems effectively (Omar & Aziz, 1996). Techniques derived from artificial intelligent research are embodied in languages or tools in order to build computer programs that closely resemble human logic. These programs would then simulate human expertise in a well defined problem domains. Expert System tools such as CLIPS is used to develop the expert system or knowledge application. CLIPS or C Language Integrated Production System was developed in 1984 at NASA's Johnsen Space Center (Omar & Aziz, 1996). CLIPS provides a complete environment for construction of rule and object based expert system.

## Internet

Internet is defined as a set of networks connected by routers that are configured to pass traffic among any computers attached to networks in the set by using TCP/IP protocols (Corner, 1997). A Network is built by connecting two or more computers, which allow the users to share facilities and information, and making more effective use of hardware (Heath, 1993; McCarthy, 1998). It is predicted that the Internet will grow to 2 billion connections in the year 2000 (Corner, 1995).

A router is the basic building block of the internet. A router is a computer that attaches to two or more networks and forwards packets according to information found in its routing table. It runs Internet Protocol (IP) in the Internet

(Comer, 1997). IP defines the format of packets used on a TCP/IP Internet and the mechanism for routing a packet to its destination (Comer, 1997). The router needs IP addresses to determine where to destination of the information. TCP or Transmission Control Protocol is a reliable and connection-oriented protocol in allowing two application programs to form connection, send data in either direction and terminated gracefully, with all the data being delivered before the termination occurs (Comer, 1998).

## Web Application

One of the many resources available in the Internet is World Wide Web or called WWW (Pabrai & Gubrani, 1996). The World Wide Web is defined as a hypertext-based tool that enables as to access and display data. The data may be in the form of text, graphics, audio or video format (Pabrai & Gubrani, 1996). Hypertext is a computer-based system for linking documents in the form of highlighted words or images and, when activated, caused the linked document to be instantly retrieved and displayed (Ford, 1995).

WWW consists of WWW browser and WWW server. As in a client/server paradigm, the WWW browser is the client. Its main function is to use the Uniform Resource Locator (URL) to retrieve document from a WWW server, interpret it in HTML and present the document to the user (Pabrai & Gurbani, 1996). URL is a syntactic form used to identify a page of information on the World Wide Web (Corner, 1997). HTML or Hypertext Markup Language is a source form used for documents on the WWW. HTML embeds commands that determine formatting along with the text to be displayed (Corner, 1997).

Examples of well-known WWW Browsers are Netscape, HotJava and Internet Explorer. Hypermedia documents displayed in the WWW Browser are known as web pages (Corner, 1997). The web pages is called hypermedia because it can contain text, graphics, video and audio clips as well as references to other documents.

As Internet gaining popularity as a source of information, web pages becoming more and more dynamic (Novak & Markiewicz, 1998). Some of the web pages trends are Database-generated Web pages , Streaming technology, Push technology, Commercial Site management programs, server and network management tools and Client-side interactivity (Novack & Markiewicz, 1998). These dynamic pages are also called web application. A web application is a specially designed and developed client/server application that uses the Internet as its network to connect between its users and server. It uses the WWW Browser as its user interface.

## Problem Statement

According to Stephen Barr in Washington Post of August, 1993 (Bacard, 1995), nearly 370 employees of the Internal Revenue Service have been investigated or disciplined for using government computers to create fraudulent tax refunds or browse through tax records of friends, relatives, neighbors and celebrities. This is one of many examples of computer crime happening around us.

The use of computer in communication and data processing is becoming more essential for the effective conduct of most business. However, this increasing dependence brings with it a significant increase in risk and threats. As the threats and vulnerability of computer systems are more clearly defined, the demand for secure products and systems is also increasing (Ettinger , 1993).

Computer data and systems have special characteristics that contribute to security concerns. Some of the important characteristics are accessibility, forgery, vulnerability and density (Carrol, 1996). Accessibility means the data and systems are more accessible at remote terminals. Forgery occurs when data in the systems are modified in an unauthorized manner and such modification cannot easily be detected and traced. Vulnerability happens when the data and systems are open to accidental and unintentional threats that can damage the data and the computer systems. Density means the data stored in computer systems are much higher than the density of any other storage media such as the print media. These characteristics increase the need to secure the data and computer systems from any security attack.

Security attacks can be classified according to quality assaulted, such as confidentiality, integrity, availability and by under siege the material which may be data or property. Such attacks could be done by nonemployees, employees or by the work of nature (Carrol,1996). The attacks are becoming easier with the use of network in distributed processing-type of computer systems. The attacker would not have to be in front of the computer to launch the attack.

However, most of the time computer system security is not considered until the operational requirements have been defined and the system is well into the implementation stage. A good level of security cannot be implemented in this retrofit basis manner. Even if the security requirements can be achieved, the costs will be quite high when compared with those incurred when the security issues and requirement are considered at the very start of the system design process. Therefore, the process of implementing security in computer systems should be considered during the definition of user requirements and incorporated to the system during the design stage (Ettinger, 1993)

In conclusion, a security system is in need to prevent computer application such as knowledge application from any possible threats. Sharing the knowledge application through the Intemet would open the application to many threats. In order to protect the valuable knowledge it is important to develop a security system which could protect such application from the possible threats.

## Objectives of Study

Objectives of this study are:

□ To design and implement an effective and practical access control mechanism to the system. This is to control which users can have access to the information system.

□ To design, develop and implement a logical access control to the information system. The concept to be used will be who can access what information and module of the information system.

## Organization of the Thesis

The thesis is organized in six chapters altogether. The chapters are Introduction, Literature Review, Theory, Methodology and Design, Result and Discussion and Conclusion.

In Chapter I or Introduction, security is defined and the need of security in application system is stressed and laid out. The topic also defined Internet and services provide to its users all around the world. One of the services which is World Wide Web is also described. Problem statement that relates to the topic of computer security and the urgent need of one comprehensive control against possible threats is also described. Lastly, the topic describes objectives of the study in details.

In Chapter II or Literature Review, reasons behind web application becoming more popular are described. Three main type of web application which are Consumer Model, Education Model and Publishing Model are defined and examples of each type are also given in this chapter. Security System and Security Services are also further described in details. This chapter gives four examples of Security System which are Pretty Good Privacy (PGP), Kesberos, Security Analysis Tools for Auditing Networks (SATAN) and Computer Oracle and Password System (COPS). In each of the security system examples, background and functions within are described. Development tool is defined as hardware and software used during the system development life cycle. Three main examples of development tools are given in this chapter. The examples are Visual Basic, Java and C++. Each of the development tolls, some background, advantages and disadvantages related to web development are described. Besides development tool, this chapter also touched on database package available for web development. Lastly, three examples are given that are Oracle, Microsoft Access and Dbase IV. Definition, functions, advantages and disadvantages of each database related to web development is described.

In Chapter III or Theory, Intemet as the fastest growing network in the history is described in great details. One of its services that are World Wide Web is also described especially its advantages in meeting current requirement of information society. Web security as one of the great concerns in the internet society is also touched in this chapter. Besides web security, information security along with its two main area, threat and security controls, and Communication Security are also defined in great details. This chapter also describes one of the most important issues in computer security that is the theory of access control and user authentication. In the effort of implementing high protection for data and computer systems, security policy of a computer system should include encryption (Madron, 1992). The theory of encryption along with three examples of cryptographic algorithm is covered in details in this chapter. The algorithm are Data Encryption Standard (DES), RSA and Intemational Data Encryption Algorithn (IDEA). In order for the system user to monitor the security of the computer system, audit trail should be embedded in the security applications. In this chapter, the theory of audit trail is described in details. Criteria of a security system and its definition are also described. Lastly this chapter gives the definition and description of Visual Basic and Microsoft Access especially in the aspect of web development.

In Chapter IV or Methodology and Design, the methodology used in designing SecureApp, which is Software Development Life Cycle or SDLC, is defined. Before the designed of the security system four prerequisite assumptions are made. The assumptions are the study of system requirement, user categories, web application that uses the security system and testing data. The general concept of security system to be designed and developed which is the SecureApp is further described in detail in this chapter before the actual design is laid out.

Feasibility study of the system is categorized into Identification of Users, Identification of Threats, and Identification of Controls and Policy to be implemented. System design consists of Identification of Process, Identification of Data Structure and Identification of System Flow. Each contents of the system design also consists of diagrams in the form of flowchart, hierarchy chart and data flow diagram. The logical design of each process in the security system is also described. The detail design and description of input and output screen needed by the security system is also included in this chapter.

In Chapter V or Result and Discussion, prototype of the security system or SecureApp is described in details. Security policy used in developing the security system is reviewed. SecureApp is divided into two main parts, which are the User Identification Module and Security Administration Module. All input and output screen for both of the module is displayed and discussed in this chapter. The connection of each of the screens with the security policy is also described in details. A screen showing the result of an encryption process is also displayed and discussed. Finally, comparison between a few well-known security systems and the SecureApp is made in this chapter. The well-known security systems are Pretty Good Privacy (PGP), Kesberos, SATAN and COPS.

Finally in Chapter VI or Conclusion and Future Work, an overall view of the security system, the important of security in software system especially web application, a brief description of methodology used in design and the usage of Graphical Usage Interface (GUI) in designing the input and output screen of the system is discussed. Limitations in the security system SecureApp are also described. Finally, the chapter discussed about future works that could be done to further enhance the security system for web application.

# CHAPTER II

## LITERATURE REVIEW

The usage of Web Application in various field is becoming more and more popular. Knowledge being an important commodity in years to come is one of the many contents of a web application. The knowledge and information could be shared among the users over the internet through a web application. The users could be limited within an organization or everybody who is connected to the Internet. In a survey reported in USA Today, electronic commerce in 1997 was estimated at $5.7 billion and is expected to grow to $117 billion by the year 2000 (Novak and Markiewicz, 1998). This is happening due to two main reasons. First, the unlimited space within the internet that allow support for huge, searchable product catalogs and allow hard-to-fine items to be sold at a low price. Second, application of the Web technology makes these systems easier to maintain compare to the real store (Novak and Markiewizc, 1998).

A consumer-type of web application normally use shopping cart system to cater the merchandise ordered by the user. Shopping card system is defined as electronic commerce metaphor for purchasing goods and services. Customers check out a virtual shopping cart, place products into it while browsing the site and pay for the accumulated items before leaving the Web site (Novak and Markiewizc, 1998).