UNIVERSITI PUTRA MALAYSIA

SECURITY STUDY AND ENCRYPTION / DECRYPTION METHOD

MAJDI TAYSIR AL-QDAH

SECURITY STUDY AND ENCRYPTION/ DECRYPTION METHOD

By

MAJDI TAYSIR AL-QDAH

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

October 2000

To my parents

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

SECURITY STUDY AND ENCRYPTION/ DECRYPTION METHOD

By

MAJDI TAYSIR AL-QDAH

October 2000

Chairman: Abd Rahman Ramli, PhD

Faculty: Engineering

Secure data transmission is done with a technology called encryption. Encryption software scrambles the data with a secret code so that no one can make sense of it while it's being transmitted. When the data reaches its destination, the same software unscrambles the information. Often the objectives of information security systems like encryption can only be achieved by following procedural techniques and abidance of laws.

This work presents an Encryption/ Decryption System that relies on a method of data rotation and XOR operations to obtain an encryption key. It uses an encryption Master Key that is a combination of both an input password Male Key and a randomly generated number called the Female Key. The decryption procedure relies on flipping of the master key to obtain the Negative Master Key

and then follows the same procedure of encryption but with a reversed Master Key. Creating the Encryption/ Decryption System was achieved by programming with Object-Oriented Pascal under Delphi 5.0 software.

Testing the system was done by taking different types of files like text, image, and video and encrypting and then decrypting them using the system. The results obtained showed that in fact the system is able to perform both encryption and decryption for all sorts of files.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluah untuk ijazah Master Sains.

KAJIAN KESELAMATAN DAN KAEDAH LERAIAN/ NYAHLERAIAN

Oleh

MAJDI TAYSIR AL-QDAH

October 2000

Pengerusi: Abd Rahman Ramli, PhD

Fakulti: Kejuruteraan

Penghantaran data yang selamat dilakukan dengan teknologi yang dipanggil leraian. Perisian leraian memecahkan data dengan kod rahsia dimana tiada siapa pun boleh mengetahui semasa penghantaran. Apabila data telah sampai kepada destinasinya, perisian yang sama akan menyatukan semula maklumat tersebut. Kebiasaannya, objektif sistem maklumat keselamatan seperti leraian hanya boleh dicapai dengan menggunakan teknik-teknik berprosedur dan hukum kepatuhan.

Kajian ini menerangkan tentang sistem leraian/ nyahleraian yang bergantung kepada prosedur pusingan data dan operasi eksklusif ATAU untuk memperolehi kunci leraian. Ia menggunakan kunci tuan yang menggabungkan kedua-dua kata laluan kunci tuan dan nombor yang dihasilkan secara rawak dikenali sebagai kunci perempuan. Prosedur nyahleraian bergantung kepada kibasan

kunci master untuk memperolehi kunci master negatif dan kemudiannya mengikut prosedur leraian yang sama tetapi dengan kunci master yang terbalik. Penciptaan sistem leraian/ Nyahleraian dicapai dengan pengaturcaraan Pascal berdasarkan objek menggunakan perisian Delphi 5.0.

Ujikaji sistem telah dijalankan dengan mengambil perbezaan bentuk fail seperti teks, imej, video dan sebagainya; kemudian menggunakan sistem leraian/ nyahleraian. Keputusan menunjukkan sistem tersebut berkeupayaan mengendalikan kedua-dua sistem leraian/ nyahleraian pada semua bentuk fail.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor Dr. Abd Rahman Ramli. This work would not have been completed without his supervision, support, and encouragement. Also, my thanks go to the members of the supervisory committee Dr. Ishak B. Aris and Dr. Sinan M. Bashi.

I would like also to extend all my thanks to the chairperson of the committee Dr. Sabira Khatun.

I would also like to express my gratitude to the staff of the graduate school for their assistance and directions in rapping up this work. My gratitude goes also to all of the individuals at the Department of Computer and Communication System Engineering who have been very supportive.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DNS	Domain Name Service
FTP	File Transfer Protocol
IP	Internet Protocol
LAN	local Area Network
NFS	Network File System
NTP	Network Time Protocol
NIS	Network Information System
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
WORM	Write Once, Read Many
WWW	World Wide Web
CGI	Common Gateway Interface
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
DES	Data Encryption Standard
RSA	Rivest, Adelman, Shamir (public key) Algorithm
X	Plaintext (text before enciphering)
Y	Cipher text (Text after enciphering)
KDS	Key Distribution Center

CHAPTER I

INTRODUCTION

Introduction to Security

Data communication is an important feature in today's society because it is the mean by which people tend to communicate and it gives the power to computers to be useful to access many sites and reach different people. Through the emerging and improving networking technology many software and information components support many systems with a variety of applications (Agnew et al., 1995).

Over the centuries, an elaborate set of protocols and mechanisms have been created to deal with information security issues when the information is conveyed by physical documents. Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve the desired result. For example, one of the fundamental tools used in information security is the signature. It is a building block for many other services such as non-repudiation, data origin authentication, identification, and witnessing, to mention few (Brickell and Odlyzko, 1988).

In the Internet, specifically, the World Wide Web (WWW) has become an important platform to access many services. It provides an effective mechanism for conveying and sharing information. The WWW is an effective method to examine and monitor remote locations because it integrates many platforms.

This brings the discussion to the security issues that the Internet and the WWW has to employ in order to secure delivering the data. Special equipment and material for specific applications are designed to protect data. In software developments new languages such as Java have made the Internet more interactive and more visual to the user in order to design a special graphic protection systems. All of this have made the security technology an important part of people's life.

Advance programs in electronics and micro-controllers have been employed to communication lines and network connections to monitor the legal access of different systems against any intrusions. So the protection of computer systems is the aim of any security procedure, which ranges from the private protection to various public protections, for example, home, business buildings and government agencies.

Objectives

The objectives of the Encryption/ Decryption System are as follows:

1. To develop an Encryption/ Decryption system for secure data transfer and usage.
2. To write the Encryption/ Decryption program using Object-Oriented Pascal Programming (Delphi 5.0).

Thesis Organization

The thesis consists of six chapters. Chapter I presents a brief introduction and objectives of the Project. Chapter II gives a literature review of general security systems as well as the encryption theoretical background needed for the Encryption/ Decryption security systems. Chapter III gives a brief introduction to the Delphi 5.0 software and Object Oriented Pascal Programming used to develop the Encryption/ Decryption system. Chapter IV presents an Encryption/ Decryption system with the program flow charts and interfaces to the Delphi 5.0 software used for the Encryption/ Decryption System. In Chapter V, results of the written programs are given. Finally, the thesis is concluded in Chapter VI by giving the summary and directions of future work.

CHAPTER II

REVIEW OF SECURITY ISSUES, GENERAL SECURITY SYSTEMS AND ENCRYPTION METHODS

Review of Security Systems

The first thing that comes to mind when mentioning security is Firewalls; a firewall is an intermediate system that can be plugged between a trusted network and the insecure Internet in order to provide a single choke point where security and audit can be imposed (Zeng et al., 1997). A firewall provides a controlled access to internet systems, concentrated security, enhanced security by hiding addresses, logging for security audits and billing, notification of security related events, integration with strong authentication keys, and policy enforcement. A firewall provides a static traffic routing service either at the network layer using screening router, or at the application level using proxy servers or application-layer gateways. Figure 2.1 shows the interaction that a Firewall does between the Host and a Network. Though very effective when dealing with some classes of attacks, firewalls fail in many cases due to their nature. A simple study of firewalls will show that they are not enough to get a network of safety because for example at the router-based level, TCP/IP package information that can be filtered is inadequate to provide the level of resolution often needed. Also, at the application level,

application-layer gateways must be built for every single application.

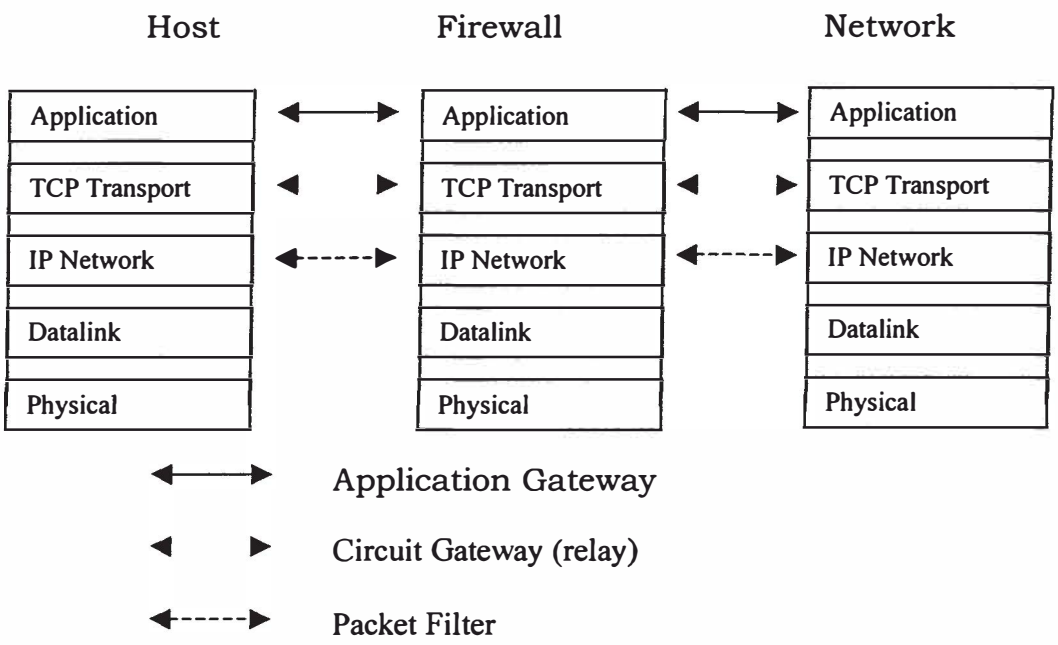

Figure 2.1: Firewall Functions as a Link between the System Host and A Network Host

Using the Internet communication lines, Encrypted Tunneling is used to provide the basis for private communications. It gives an Authenticated and Encrypted connections and a free of modifications normal working applications. For a secured network, an essential point-to-point communication must be guaranteed. To safeguard the open network as the Internet, it must provide authentication and data confidentiality services to both the sender and the receiver. Encryption has been successfully used to achieve the confidentiality. DES (Data encryption standard) is the present prevailing standard on Internet among hundreds of algorithms

and protocols. Authentication, based on the technologies of encryption, is well established and used. To expand security from *point to point* communication to multi-node open network, a lot of parameters should be added for consideration. Figure 2.2 shows where Encryption and Authentication lie in a system security. Since encryption is the basis of *point to point* communication security, the issue of how to manage encryption keys in open network has become a hot topic. KDS (Key Distribution Systems) systems; which are to establish and store keys, and distribute them to network resources requesters, have been developed in succession, e.g. MIT's Kerberos and IBM's KryptoKnight (Brown et al., 1990). Access control mechanism, which determines user's access authority, play a key role within KDS systems. Both of the above mentioned KDS systems are weak in this respect. For example, Kerberos relies heavily on static and one-time check of user's ID and password, thus providing a so-called 'All or nothing' mechanism, which is somehow easy to be penetrated. On the other hand, while cryptography is valuable for Internet security, it is not a feasible way to control access to documents. Cryptography can only control secrecy and authentication aspects, but cannot handle different types of access by different users, access to portions of documents, and other content restrictions (Anand et al., 1997).

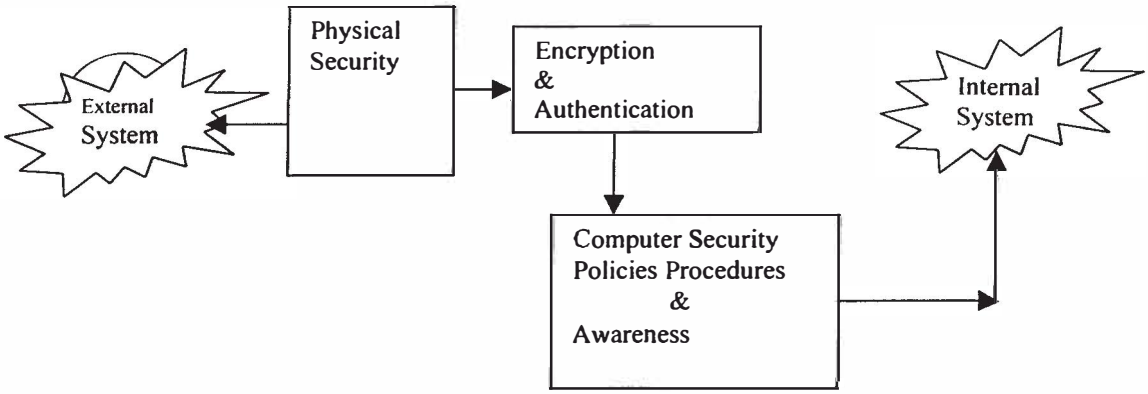

Figure 2.2: An Integrated Security

Rangachari, et al., (1997) presented a protection domain system for downloading content dynamically over the Internet. In this system, downloading principals retrieve content and content stamps that attach descriptive information to content in a secure manner. The system architecture uses content stamps to authenticate content and derive its protection domain. The content stamp specifies the authentication information and execution requirements of the content from the manufacture's and/or rating service's viewpoint. The architecture is designed to utilize such information, as well as user input, to determine the content's protection domain. The domain enforcer must determine which content is being executed and enforce the appropriate protection domain upon it.

Baraka, et al., (1998) presented a new model of Intranet security that is connected to the Internet based on a hybrid model

technique; the new model integrated the Prevention model (Firewall) and the Detection model (Intrusion Detection System).

Zeng, et al., (1997) proposed an Internet Security System for only one network domain (subnet); four kinds of agents are deployed in the system. They are User agent, Domain Security Agent (DS Agent). Access Control Agent (AC Agent), and Audit Agent. A Security Information Repository was used to store security information for network domain, including access information, user profiles, application profiles, authentication keys, etc. These agents communicated to each other through the Information Broker which runs as a co-ordinator not only for the security agents but also for all of the accessible applications in the subnet. A firewall was used as the interface between the subnet and the Internet. Its main function is to filter out the requests which intend to bypass the *Information Broker*. Additionally, in order to handle the requests from users in other subnets, agents may contact through Internet with their peer agents in the remote network. This system integrated many available technologies such as firewall, authentication, encryption, and access control, etc. By which is able to provide a somewhat comprehensive and overall solution.

Dauerer, et al., (1997) described a system called the Web Access Control Front End (WACFE) for managing security on

World Wide Web applications. The system provided a method for managing the security of applications consisting of many files located in many directories with a minimum of effort on the part of the system administrators.

So this brings the discussion to what the security protocols and systems are being developed to do. Securing data actually is the objective of any security system. All the above systems were designed in order to secure delivering the data or storing them in addition to managing and manipulating them. Encryption has been used and implemented for a long period of time to do just that: protect the data while in mobile and while being stored in server locations. Encryption is changing of the actual data to something that is not the original so that if being intercepted, the interceptor will not be able to use the data.

Encryption

Suppose that someone wants to send a message to a receiver and wants to be sure that no one else can read the message. However, there is the possibility that someone else opens the letter or hears the electronic communication. In cryptographic terminology, the message is called plaintext or cleartext. Encoding the contents of the message in such a way that hides its contents from outsiders is called encryption. The