EXAMINERS COMMITTEE

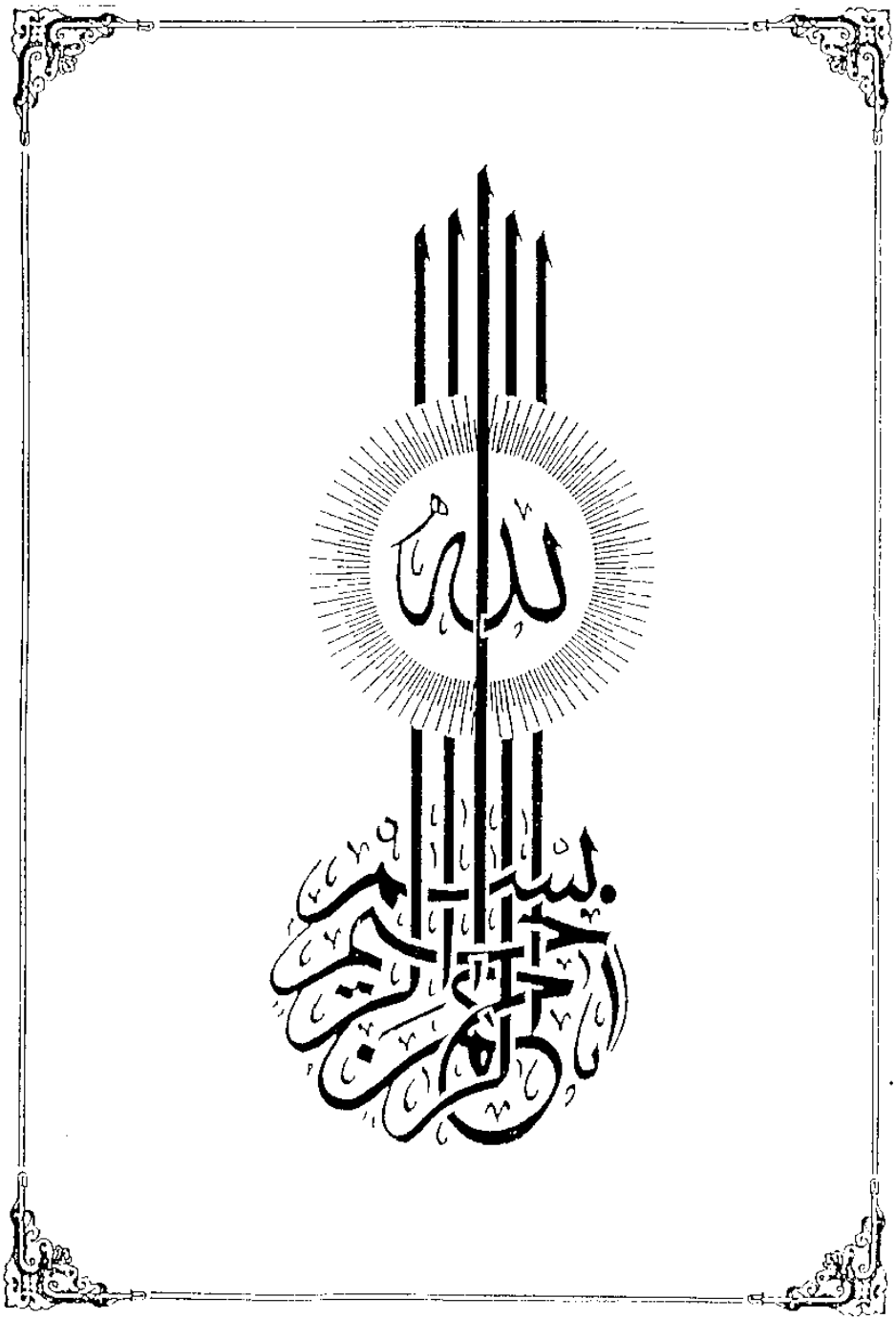
Name, Title & Affiliation **Signature**

1- Prof. Dr. M. Zaki
Prof. of Computer Science,
Computer Engineering Department,
Faculty of Engineering,
Al-Azher University.
Cairo

2-Prof. Osman Badr
Prof. of Computer Systems,
Computer & Systems
Engineering Department,
Faculty of Engineering,
Ain Shams University.
Cairo

3- Prof. Dr. M. Adeeb R. Ghonaimy
Prof. of Computer Systems,
Computer & Systems
Engineering Department,
Faculty of Engineering,
Ain Shams University.
Cairo

To
Tahany,
Ahmed, and Reham
and
the memory of my Mother and Father



STATEMENT

This dissertation is submitted to the faculty of engineering, Ain Shams University for the Degree of doctor of Philosophy in Computer & Systems Engineering.

The work included in this thesis was carried out by the author in the Department of Computer & Systems Engineering, Ain Shams University, From January 1988 to November 1994.

No part of this thesis has been submitted for a degree or a qualification at any other University or Institution.

Date :
Signature : 
Name : Bahaa Eldin Mohamed HASSAN

ACKNOWLEDGMENTS

Like most dissertations, mine has taken a long time to be finished. So it seems more than appropriate to acknowledge and to thank those who have helped me to write it and those who have helped me to survive the writing of it.

I would like to acknowledge my deepest gratitude and thankfulness to **Prof. Dr. M. Adeeb R. Ghonaimy** for his valuable supervision and for his invaluable help during the preparation of the thesis.

I would like to express my deepest gratitude to **Dr. Fathy S. Holail**, who suggested the subject of this thesis. I am also most grateful to him for his fruitful guidance, invaluable advices and technical support to develop my ideas for secure communication network.

I am greatly indebted to **Prof. Shigeo Tsujii** of Electronic Engineering Department, Tokyo Institute of Technology, Who provide me with all facilities he has at his laboratory to develop and implement a part of this work. Also my due thanks go to all his lab staff members.

I wish to express my deepest gratitude to **Prof. Matar Ali Matar** for his stimulating discussion, invaluable comments and sincere advices during the preparation of this thesis.

Preface

–One of the landmarks of this era is the establishment of means of accessing and updating computer based Information and broadening of the availability of computer resources. Data and computer communication networks are the concrete materialization of the intended means. Over such networks computer time sharing, financial transactions, bulk transfers...etc., are realized. Legal and illegal operations are possible over such networks as they are wide open multi-user environments.

Network resources are subjected to illegal access by intruders through passive as well as active attacks. Success of such attacks results in some form of:

- Unauthorized release of information.
- Unauthorized modification of information. (only active attacks do).
- Unauthorized denial of use of resources (only active attacks do).

This necessitates that a security policy have to be adapted and counter measure have to be taken or incorporated in hardware and software of the computer network. This include:

1- Conceal mint of information over the network (stored or communicated) by encryption techniques.
2- Positive identification of all users and authentication of their identities as well as attachment of unforgeable identifiers to all programs being processed.
3- Isolation of users and their processes from each other and from supervisory and system control programs.
4- Implementation of effective integrity control and auditing procedures.

These points are more or less belonging to what is known as internal protection mechanisms as distinguished from other mechanisms dealing with the user administration controls, hardware and software protection mechanisms

Effectiveness of incorporated security mechanism have to be assessed, evaluated and rated (or ranked) on the basis of satisfaction of prescribed security criteria. This entails the elaboration and validation of a convenient security model

This dissertation addressed the question of security a PC-based computer network without impairing its performance and transparency. A representative network is assumed to incorporate several hosts; each has its own star-connected terminals the assumed communication medium is the public switching telephone network.

The required network security features:

1- Powerful data encryption scheme for both file as well as communication security.
2- Protected access control.
3- User and message authentication.

4- Digital signature scheme.
5- Compatibility of the add-on facility to I/O slot specifications to allow "portability" to all IBM-PC platforms.

Chapter 1 presents the aspects of the computer network security. Firstly several classification of networks are outlined with emphasis upon task protocol based classification exemplified by OSI, TCP/IP, SNA and DNA architecture. Secondly, the network security problem is introduced along with relevant counter-measures and services. Security evaluation criteria and models are highlighted. Finally related works are summarized.

In chapter 2 The computer system incorporated security mechanisms are considered. Protection of data by encryption end-to-end basis is presented. Several authentication and digital signature techniques are given. Moreover, the access control problem is outlined. This mechanism serve as the basis for defining the features and concretizing the implementation of the proposed system in chapter 3.

Chapter 3 presents the main contribution of the thesis. For the defined configuration of the network, implementation of access control, authentication, digital signature and encryption functions is given and operated satisfactorily

Encryption is done on the basis of a patented Vernam-like scheme and a personalized hardware using programmable logic devices.

Access control adapts a smart card philosophy in conjunction with a developed software. As to authentication and digital signature, a software package is developed to implement their function and to manage the whole system operation. Pseudo code implementation of algorithms is given in the appendices. In fact the thesis has several appendices covering hardware and software details.

Chapter 4 is devoted to evaluation of the proposed system. System performance costs in terms of delays (due to overheads and handshaking procedures) are considered. Usability and transparency of the system have been demonstrated. Relative ranking of the system is presented. Moreover, ranking or rating on the TCSEC basis is considered.

Chapter 5 Contains the conclusions and future work proposals. The main outcome of this work is the built and proven security computer network. Speeding up the system may be considered are the main issue for work extension.

ILLUSTRATIONS

Figures

Tables

CONTENTS

CHAPTER 1

Chapter 1

INTRODUCTION TO COMPUTER NETWORK SECURITY.

1.1 Overview of Computer networks

A system in which a large number of separate but interconnected computers, perform a job is called a "Computer Network" [TANE 89]. Its goals are :

- To make all programs, data, and other resources available to any one on the network without regard to the physical location of the resource and the user.

- To provide high reliability by having alternative sources of supply.

- To reduce the costs, small computers have a much better price/performance ratio than large ones, so it becomes attractive to build systems consisting of powerful personal computers, one per user, with data kept on one or more shared file server machines., and only communicate with other computers when needed.

- To provide a powerful communication medium among widely separated users. This means that it is easy for two or more people who live far apart to write a report together.

•Computer Networks can be classified as follows:

According to localization of processing power

–Centralized Computer Network. Where the processing power is centralized in one location. The terminals can only communicate with host (1st wave of computer networks).

–Distributed Computer Network (Processing power is distributed geographically).
•Hierarchical (Direct communication is not granted for all processors) (2nd wave of computer networks)
•Peer-to-peer (Direct communication is possible between any two processors) (current trend in computer networks)

According to network topology

–Point-to-point Networks (suitable for long distances).
•Star
•Mesh

–Broadcast Networks (suitable for short distances).
•Bus
•Ring

According to Geographical coverage area

•Wide Area Network (WAN).It is between continents, where the transmission facilities are provided by common carriers. This include: satellite, coaxial cables, public data networks, and public telephone networks. (Data rates typically are low)

•Regional Area Networks (RAN). It is between countries in same region. The transmission facilities are provided by common carriers. (Data rates typically are low)

•Metropolitan Area Networks (MAN). It is between large metropolitan cities. The transmission facilities are provided by common carriers. (Data rates typically are high)

•Local Area Networks (LAN). It is within one building or between group of neighboring buildings (e.g. offices, and university campus) where transmission facilities are provided by user. (Data rates typically are high).

According to Switching principles

•Public Switched Telephone Networks (PSTN)

Circuit-switched WANs establish a dedicated physical circuit through the network between a source and a destination just as with a telephone call. The subnetwork intermediate nodes in the early days were electro-mechanical switching devices. Data is transmitted as analog signals through the subnetwork over dedicated telephone channels at data rates up to 20 k bps.
The major disadvantages of this are

(1)both the source and destination have to be available at the same time,

(2)some proportion of the available capacity (bandwidth) of the subnetwork is reserved in advance,

(3)users typically pay for connect time rather than volume of data.