UNIVERSITI PUTRA MALAYSIA

COMPUTER COMMUNICATION NETWORKS SECURITY ANALYSIS

LAWAN AHMED GUMEL

FSAS 1999 2

COMPUTER COMMUNICATION NETWORKS SECURITY ANALYSIS

By

LAWAN AHMED GUMEL

Thesis Submitted in Fulfilment of the Requirements for the Degree of Master of Science in the Faculty of Science and Environmental Studies Universiti Putra Malaysia

May 1999

DEDICATION

TO MY PARENTS

ACKNOWLEDGEMENTS

During the preparation and the development of this study, help has come from innumerable people, and to this collectively I express my thanks. Thanks especially to my committee members: Dr. Noor Akma Ibrahim, and Assoc. Prof. A. K. Ramani for their invaluable editing corrections/advice that brought the thesis to completion. My special thanks go to Assoc. Prof. Harun Budin for encouraging the research work from its inception.

I wish to express special gratitude to Dr. Leow Soo Kar, the Chairman of the Supervisory Committee for his keen interest, valuable contribution, tireless guidance and encouragement throughout the undertaking of the research work.

Sincere appreciation goes to my family particularly my parents for their love, care, and spiritual support through their fervent prayers. The help of my Uncle Alhaji B. M. Gumel cannot be given a passing comment.

I am greatly indebted to the entire staffs of the Mathematics Department for their diverse cooperation. The hospitality of the Malaysian is gratifying.

Finally, I would like to thank: Dr. Inuwa Shehu Usman, Dr. Idris Bugaje, Dr. Suleyman A. Muyibi, Mallam Nasir Umar Tsafe, Mallam Usman Ghana, Idi Fulaye for their support and advice.

Praises and thanks to Almighty ALLAH for the wonderful guidance, good health and direction (Alhamdulillah).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure **Page**

LISTS OF ABBREVIATIONS

ATM	Asynchronous Transfer Mode
ANS	Advanced Network Service
ARPA	Advance Research Projects Agency
AIS/NET	Advanced Information Systems Network
BNA	Burroughs Networks Architecture
CA	Corrective Action
CBC	Cipher Block Chaining
CPU	Central Processing Unit
CSNET	The Computer Service Research Network
CMST	Capacitated Minimum Spanning Tree
CFA	Capacity Flow Assignment
CPEs	Customer Premises Equipment
CCITT	International Telegraph and Telecommunication Consultative Committee
DES	Data Encryption Standard
DECNET	Digital Equipment Corporation Network
DNS	Domain Name System
DTEs	Data Terminal Equipment's
EDI	Electronic Data Interchange
EMS	Electronic Meeting System
EFT	Electronic Fund Transfer
GOC	Group Oriented Cryptosystem
IBM	International Business Machines Corp.
KAC	Key Authentication Center
KDC	Key Distribution Center
LAN	Local Area Network
MAN	Metropolitan Area Network
MD5	Message Digests Algorithm
MCI	Microwave Communications, Inc.
MIC	Message Integrity Code
MSN	Manhattan Street Network
MST	Minimum Spanning Tree

MTA	Mutually Trusted Authority
NSF	National Science Foundation
NMC	Network Management Control
OS	Operating System
PEM	Privacy-Enhance Message
PGP	Pretty Good Privacy
RSA	Rivest Shamir Adleman
SNA	Systems Network Architecture
TC	Trusted Center
TCP/IP	Transmission Control Protocol/Internet Protocol
UA	User Agent
UTP	Unshielded Twisted-Pair
WAN	Wide Area Network

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

COMPUTER COMMUNICATION NETWORKS SECURITY ANALYSIS

By

LAWAN AHMED GUMEL

May, 1999

Chairman: Leow Soo Kar, Ph.D.

Faculty: Science and Environmental Studies

We are living in the "Information Revolution", where development of powerful communication systems and digital technologies have resulted in the buildup of massive information banks by government, industries and even individuals, which are required to be protected to maintain privacy, confidentiality, availability and integrity of national and commercial information. It has also allowed for automation of services and such systems must protect customers against modern day "electronic crimes". The first part of this thesis is a study into the aspect of the development of secure communication between group of entities. The thesis gives an overview of the general issues that are raised by the concept of cryptosystems, followed by discussions on the methods currently available for the conduct of such techniques. Generic categories of threats and vulnerabilities to computer networks are outlined as well as network security objectives. The study culminates in the description of a recommended alternative approach for the development of Group Oriented Cryptosystems (GOC) which can be used to solve the problem of entity authentication and subsequent key distribution in order to enhance multiple-entity (group of entities) communications with confidentiality and integrity services.

E-mail security is about protecting electronic mails from spies, interlopers, and spoofs. People who may want to destroy, alter, or just look at our private communications. The second part of the thesis shows how we can protect the financial information, contract negotiations, or personal correspondence we entrust to public or private networks by means of *Digital Envelop*. Furthermore, the model developed can be practically implemented.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
Sebagai memenuhi keperluan untuk ijazah Master Sains.

ANALISIS KESELAMATAN RANGKAIAN KOMUNIKASI KOMPUTER

Oleh

LAWAN AHMED GUMEL

Mei, 1999

Pengerusi: Leow Soo Kar, Ph.D

Fakulti: Sains dan Pengajian Alam Sekitar

Era "Revolusi Maklumat" terkeni memperlihatkan bagaimana pembangunan sistem komunikasi yang teguh berserta dengan teknologi digital telah menghasilkan pembinaan bank maklumat yang gergasi oleh pihak kerajaan, industri serta para individu. Justeru itu perlindungan untuk memelihara kerahsiaan, keyakinan, kesediaan dan kewibawaan maklumat nasional dan komersial diperlukan. Kedua-dua ini juga telah membenarkan sistem layanan secara automasi yang mana sistem seperti ini perlu melindungi pelanggan daripada "jenayah electronik"zaman moden. Bahagian pertama tesis ini meliputi kajian mengenai aspek pembangunan komunikasi keselamatan diantara beberapa entiti. Tesis ini juga memberikan secara keseluruhan isi umum yang timbul dari konsep kriptosistem, diikuti dengan perbincangan keatas kaedah yang tersedia ada untuk mengendalikan teknik kriptosistem ini. Rangkaian komputer sentiasa terdedah dari beberapa ancaman dan berada dalam keadaan bahaya. Justeru itu beberapa kategori ancaman generik dan keadaan bahaya ini disenaraikan. Juga digariskan objektif keselamatan rangkaian. Suatu pendekatan alternatif bagi membangunkan Kumpulan Berorientasikan kriptosistem disarankan. Kaedah ini boleh digunakan untuk menyelesaikan masalah ketulinan entiti dan taburan jujukan kunci. Yang demikian keyakinan dan kewibawaan terhadap layanan komunikasi entiti berbilang akan meningkat.

Keselamatan e-mail memperihalkan perlindungan mel elektronik daripada pengintip, orang yang tidak berkenaan dan penipu yang mana mereka ini mungkin ingin menghapus, menukar atau mencerobohi komunikasi sulit kita. Bahagian kedua tesis memperlihatkan bagaimana kita boleh melindungi maklumat kewangan, kontrak perbincangan atau rangkaian sulit ini melalui *Selubungan Digital*. Selanjutnya model yang dibangunkan boleh dilaksanakan secara praktik.

CHAPTER I

INTRODUCTION

The idea that we are living in a new era, in which our economy, society, culture and political life are increasingly shaped by computers and communications, goes back about forty years. In the past years a series of remarkable developments have confirmed that Marshall McLuhan was right " we are living in a global village" (Donald, 1990). Computer and communication technologies are indisputable at the heart of many strong forces that are reshaping the world and our perception of it.

The fields of telecommunications and networking have, in particular, witnessed more significant developments than many other fields of human knowledge. This is primarily due to the fact that telecommunication is the engine that is driving the information age into our daily lives, as compared to the forces that brought us the agricultural and industrial ages earlier. Telecommunications and networking have been growing at an explosive rate, and all indications are for their continued growth. Some of the major factors influencing this phenomenal growth are technology driven. Developments such as fiber optics, Local Area Networks (LAN), Wide Area Networks (WAN), digital and switching techniques and satellite technology have all contributed towards reduction in the cost of communication. Globalization of business services and the need to coordinate manufacturing, marketing services, and financial activities over large distances are also contributing to the importance and growth of telecommunications and computer communications. Many corporations have discovered the use of telecommunication-based system and computer networks for their transactions. Furthermore, it will enable a firm to build strategic information resources that

allows it to take advantage and to confront competitive forces in the market. Growth will continue in electronic mail systems (Harper, 1989). Similar observation have envisaged in electronic data interchange (EDI), voice-mail, facsimile, electronic meeting systems (EMS), teleconferencing, telecommuting, electronic funds transfer (EFT) and various electronic communications systems (O'Brien, 1993). These developments have increased the market size which, in turn, have contributed to price reductions.

The Need for Computer Networks

Networks satisfy a broad range of purposes and meet various requirements. Some of the common objectives of computer communication networks are:

1. Cost savings, greater availability of software, easier use and maintenance as well as higher performances.

2. Sharing of (distance) resources such as information (databases) or processors (CPUs). Modern organizations today are widely dispersed, a network provides the means to exchange data among computers at a diverse part of a country and the world, and to make programs and data available to the diverse workers of the enterprise.

3. To provide interprocess communication, such as among users (or processes) and processors, or the work on one computer can be reloaded through the network onto another computer in the network.

4. To improve reliability of networks through redundancy. Networking also supports the critical function of backup in case a computer fails or malfunctions, the backup computer can then take over.

5. Distribution of processing functions. For example, a transaction is translated in one node, processed in another, and the response formatted in a third node.

6. Furnish central control for a geographically distributed system, such as inventory management in the manufacturing industry, managing prices and sales, and handling accounts etc.

7. To provide centralized management and allocation of network resources: host processors, associated databases, transmission facilities, and the like.

8. It provides compatibility of dissimilar equipment and software.

9. It also provides an efficient means of transporting large volume of data among remote locations. The use of networking allows a very flexible working environment. Employees can work at home by using terminals linked through networks into the computer at the office.

Computer and Network Security

We will first examine alternative definitions of computer security and then narrowing the definitions toward more formal definition.

Valuable information of any kind needs protection from unauthorised access and/or alteration. In the case of computer data, this means more than placing a padlock on a door.

In the early days of computing, computer security was of little concern. The number of computers and the number of people with access to those computers was limited (Amoroso, 1994). The first computer security problems, however, emerged as early as the 1950's, when computers began to be used for classified information.

Confidentiality (also termed secrecy) was the primary security concern, and the primary threats were espionage and the invasion of privacy. At that time and up until recently, computer security was primarily a military problem, which was viewed as essentially being synonymous with information security. From this perspective, security is obtained by protecting the information itself.

By the late 1960's, the sharing of computer resources and information, both within a computer and across networks, presented additional security problems. Computer systems with multiple users required operating systems that could keep users from intentionally or inadvertently interfering with each other (Garfinkel and Spafford, 1996). Network connections also provided additional potential avenues of attack that could not generally be secured physically. Disclosure of information was no longer the only security concern. Added to this was concern over maintaining the integrity of the information. Conventional wisdom dating from this period was that governments are primarily concern with preventing the disclosure of information, while businesses are primarily concerned with protecting the integrity of the information, although this is becoming less the case (Amoroso, 1994).

Defining Computer and Network Security

In their popular text on Internet security and firewalls, (Cheswick and Bellovin, 1994), define computer security to be "keeping anyone from doing things you do not want them to do to, with, on, or from your computers or any peripheral devices." Using this definition, computers are seen to be targets that can be attacked ("do to"), or tools that can be used ("do . . . with, on, or from"). From this perspective, computer security is distinguished from information security. "Computer security is not a goal, it is a means toward a goal: information security.

A more operational definition is presented by (Garfinkel and Spafford, 1996) in their text on Unix and Internet security: "A computer is secure if you can depend on it and its software to behave as you expect . . . . This concept is often called trust: you trust the system to preserve and protect your data." The authors intend for this definition to include natural

disasters and buggy software as security concerns, but to exclude software development and testing issues.

These definitions are relatively informal, and as a result, they are not adequate to the development of a taxonomy of computer security problems. Ideally, a definition would unambiguously demarcate the boundaries of the field of concern. For example, natural disasters and buggy software both can result in damage to computer files, and therefore, a very broad definition of computer security would include both of these. As a practical matter, however, the computer security field is not usually considered to be this inclusive. Garfinkel and Spafford include these concerns in their definition of computer security, but they narrow their focus on "techniques to help keep your system safe from other people – including both insiders and outsiders, those bent on destruction, and those who are simply ignorant or untrained."

Narrowing the Definitions

There are many events that could result in damage to or loss of computer files that are included in the broad, informal definitions of computer security, but they are more appropriately considered as part of related security fields. Theft of computer equipment would certainly result in the loss of computer files, but this type of theft is similar to the theft of the copy machine, telephone, jewelry, or any other physical object. Methods to provide security for physical objects are well developed and are not unique to computer equipment. Environmental threats, such as earthquakes, floods, lightning, power fluctuations, humidity, dust, varying temperatures, and fire, can also result in damage to computer files, but they also can cause damage to other property. It seems customary for authors to include these threats within their broad computer security definitions, but they then proceed to exclude discussions

of these problems in their texts or papers on computer security. The definition of computer security developed here is intended to explicitly exclude these areas.

Another similar area involves software. "Buggy" software is certainly a threat to computer files. Improperly implemented software could cause files to be damaged or lost. But this does not, of course, mean that we should include software development as a subset of the computer security field. Most software development issues, instead, fall outside of the computer security field. Software errors, however, clearly lead to security problems: they sometimes create vulnerabilities that can then be exploited. In fact, software that operates correctly can also be a security problem when it is operated in a manner not intended.

A common method to narrow the definition of computer security is to concentrate on the three categories of computer security. According to (Chales, 1996): Computer security consists of maintaining three characteristics: Confidentiality, Integrity, and Availability.

Confidentiality requires that information be accessible only to those authorized for it, Integrity requires that information remain unaltered by accidents or malicious attempts, and Availability means that the computer system remains working without degradation of access and provides resources to authorized users when they need it. However, in recent years, more and more reported instances of computer system vulnerabilities and attacks have been recognized or noticed that cannot be easily associated with one of disclosure, integrity, or denial of service (Amoroso, 1994).

Moreover, this concentration focuses computer security on the protection of computer files, and ensuring the availability of the computer and network system. This focus is too

narrow for at least two reasons. First, many attackers indeed are attempting to use process access to gain access to files, but many are simply after the process access itself.

The other reason this focus is too narrow is found in the security architecture of Unix-based computer systems, where security is based on protection of objects, which includes both processes and files. Access to processes is commonly restricted by accounts to which the user must log in, such as by entering the correct user name and password. Once an attacker gains access to a process, then the process must be used to gain access to files. In other words, access to a file system requires two steps: access to a process, then access to the file. This is illustrated by a typical Unix process, such as the */bin/cp* utility (used to copy files). A user gets access to this utility upon successfully logging into an account. Access to the */bin/cp* utility, however, does not mean that the user can now use this process to copy any file. When a process runs, it may access only a limited collection of files that are associate with the user (Tanenbaum, 1992). The user may, therefore, use the */bin/cp* utility only to copy files for which that user has the appropriate permission.

In addition to using processes to access files, processes may also be used to access data that is in transit across a network. In this case, these data are not contained in files which would be located in primary memory (the computer's volatile random-access memory), or in secondary memory (storage disks). They are instead a stream of data packets in transit. These can be accessed by processes operating at the origin host for the data transmissions, at the destination host, or at hosts in between through which the data pass.

In summary, conceptualizing computer security as being based on providing confidentiality, integrity, and availability in a computer system narrows the focus to the *files* in a system. Confidentiality and integrity specifically refer to the prevention of disclosure,

alteration or deletion of the information contained in computer files. As discussed above, however, this is only one of the levels of access in a typical computer security system. Access controls are used to restrict access to processes, files, and data in transit.

The Need for Secure Networks

A secure network is critical for the survival and success of many businesses, as it has become an integral part of businesses, and it is hard to separate the risks to networks from the risks to the businesses. This accelerating growth on networks has vastly exceeded the corresponding improvements to ensure their security. Moreover, it also continues to expose new loops and vulnerabilities in network security issues. Many security attacks take place on networks. Ryan and Bordoloi (1997) reported that conservative estimates of annual losses due to security breaches stands at about US $80 million. Some survey firms indicate that the losses may actually be in billions of dollars, they also indicated that another study shows that a single breach in security can cost hundreds of thousands of dollars. Ahuja (1996) reported that, according to the Computer Emergency Response Team at Carnegie Mellon University, they receive an average of three new computer security incidents every day. They presented some startling statistics, that by January 1995, the number of viruses had increased to approximately 6000, a 40% increase in 12 months. According to (Dr. Solomon, 1998), the number of viruses now (1998) is more than 20,000 (refer to Chapter II for details). In 1992, cheque frauds cost the financial services industry over US $1 billion, while credit card fraud cost the industry over US $3.5 billion. The number of reported hacker invasions increased from 252 in the year 1990 to 2341 in the year 1994. While downtime at a major banking data center cost approximately US $5000 per second, yet the total loss resulting from security breaches is still unknown.

Some Statistics

- The FBI estimates that there is a US $7.5 billion annual loss to electronic attack.
- According to the Wall Street Journal 21/8/95, "Russian computer hackers successfully breached a large number of Citicorp corporate accounts stealing US $400,000 and illegally transferring US $11.6 million"
- The Times of 3/6/96 reported that hackers had been paid £400 million in extortion money to keep quiet about having electronically invaded banks, brokerage firms, and investment houses in London and New York with 'logic bombs'.
- US department of defense report found that 88% of their computers were penetrable. In 96% of the cases where their tiger teams got in, the intrusions were undetected. Note that the DoD are really seriously concerned with security.
- In 1984, a bank funds transfer netted $25 million for a branch manager who manipulated a computer system by entering offsetting entries that evaded auditing (Rusell and Gangemi, 1991).

Electronic Mail

Electronic Mail is an electronic communications system that is used to send information from one person/site to another (one-to-one communication), or from one to many people at the same time (called broadcasting or one-to-many communications). Depending on the system used, electronic messages can comprise data, text, audio, or graphic information. However, unlike regular letters that are written on paper and sent via the postal service, “electronic letters” and “electronic packages” are entered into a terminal and then transmitted electronically, arriving almost instantaneously instead of taking a day or more to reach their destination. Electronic mail facilitates communication and information exchange in a multitude of ways and touches every aspect of the communications industry.

E-mail is not the only form of electronic messaging. The telephone is another, as is the facsimile (fax) and telex. Each of these forms can operate independently. Individuals use E-mail because it is fast and reliable, and sometimes even because it is cheaper than a long-distance telephone call. However, the E-mail cost mentioned does not include whatever amortized cost there would be of the terminal or computer to send the message or the portion of the telephone costs that could be shared.

E-mail will not be the only form of communication in the future, of course. Nor will it be the only form of mail. Different media have different strengths, so many will survive. Paper mail, or "snail mail" "s it is known to E-mail enthusiasts, will still be ideal for conveying a personal, concrete touch. Voice calls and voice mail will carry intonations and emotion that E-mail cannot match; fax machines will print a letter even where there is no computer to receive E-mail, and so on.

Reasons for E-mail

E-mail has come a long way since it was the plaything of bearded researchers working the midnight shift in university computer centers. Companies have adopted it all over the world, to connect people inside the company to one another as well to those outside the company. In fact, some studies show that the number of business E-mail messages are increasing exponentially. Imagine a business without telephones. This is practically impossible. Many analysts think E-mail will become equally as basic to business as telephone. E-mail could become a main corridor to move information such as job orders, personal instructions, and engineering suggestions.