A SURVEY ON DATA SECURITY & COMPUTER NETWORKS

MR. SHASHIRAJ TEOTIA (MCA, M.TECH (IT), *Ph.d(cse))*

MR. RAVI PUNIA**

Mrs. MONISHA AWASTHI**

Abstract:

This research deals with data security in distributed and client/server computer systems, placing special emphasis on access security.

The paper presents the subject of data security & computer Networks in these systems by describing them, examining their vulnerable points and presenting adequate solutions. The paper includes a survey on the subject of authorization, authentication, encryption and access control, the main components in data security management of distributed systems.

In addition to a survey and analysis of data security management aspects, a plan of an access security system based on client/server architecture is presented, which may be combined with applications requiring access security services. The model describes the access security server and the interface for access security which is combined with the application and constitutes the client portion.

Unlike research carried out to date which mainly integrates existing techniques and approaches (White 1999, Burleson 1998, Gayness 2000)? This research offers an innovative approach on the subject of data security management through the development of a unique access security Model. Furthermore, in view of the increasing importance and intensive use of data security management

* Assistant Professor (Department of Computer Application), Swami Vivekanand Subharti University, Meerut.

** Assistant Professor (Department of Computer Application), Adharshila College of Education, Meerut.

technology, and the special attention paid to the various aspects connected with data security management, this research is of special importance from the theoretical and applicative points of view.

Keywords: Distributed computer systems, aspects of Client/server systems, The Distributed Security Approach, Application the Layered Design in Data Security, Conclusion.

Introduction:

Every organization should be concerned about protecting data against intruders, for the organization's ability to survive depends on the availability, comprehensiveness and reliability of its financial and organizational data.

Security has become more complicated with the expanded use and networking of personal computers. At present, the local networks and the connections between the large and small computers are such that each of them takes part in the application.

The application as a whole appears to be located on the user's computer, but in fact each user and each application has access to, and sometimes even control over, organizational data on various computers and storage facilities. Obviously, such openness invites unauthorized use, and requires data security coordination and management (Appleton, 1997).

Unfortunately, many companies do not deal with data security and network management problems until there is a crack in the network. To protect vital information, the companies must set up a sound security system before the network is intruded. This involves identification of the security risks, applying sufficient means of security, and teaching the users data security awareness.

1. DATA SECURITY:

In simple terms, the Data security is a practice of keeping data protected from unauthorized access & corruption. The focus behind data security is to ensure privacy while protecting personal or corporate data.

1.1 Security system components in - Distributed computer systems

Distributed computer systems pose four main securities components: security authentication, authorization, access control and encryption.

- **Authentication –** Usually authentication is realized by a "smart token" which is a hardware device in the size of a pocket computer or credit card that creates a password and transfers it to the authentication server that is linked up to the network.

- **Authorization -** The aim here is to supply one secured access point enabling the users to link up to the network once and allow them access to authorized resources.
  The authorization is examined via software servers enabling the client, acting in the name of the user, to prove his identity to the authentication server, without sending information over the network that would reveal the client or the party rendering the service.

- **Encryption -** Implemented using intricate algorithms such as RSA, PGP, DES based on the use of public and private key systems (Fleeter, 1997).

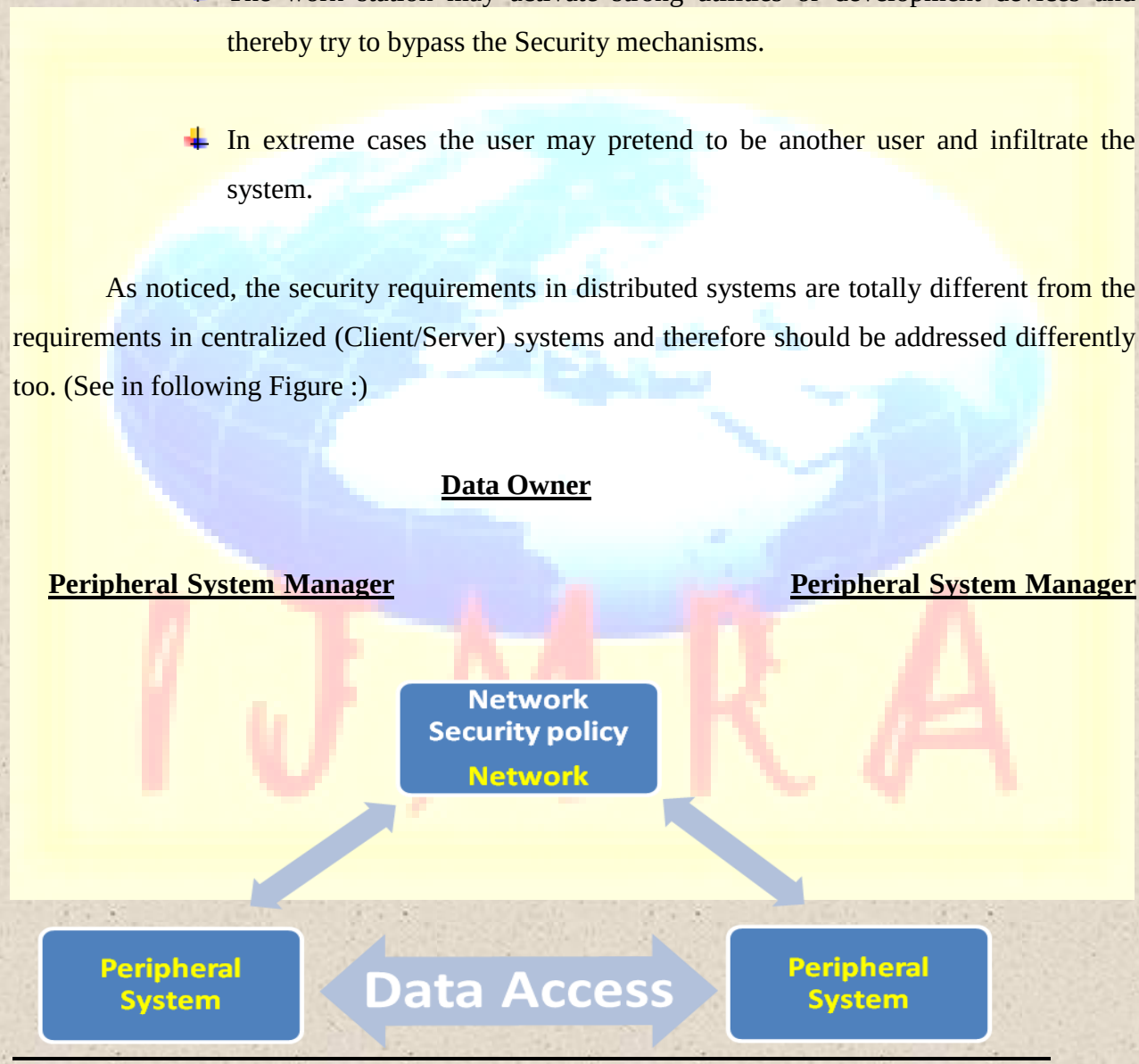
- **Access control -** Implemented via access matrices, access lists, capabilities list. These lists define access authorization to the computer resources for the user.

1.2 Data security aspects of- Client/server systems

From a system manager point of view it is possible to point out the following threats from distant stations in client/server systems (Appleton, 1997; Gayness, 2000):

- The work stations approval mechanism of the users may be partial or non-existent.
- It is possible to carry out automation of the Login procedure.
- The work station may be installed in a public area or in a high risk area.
- The work station may activate strong utilities or development devices and thereby try to bypass the Security mechanisms.
- In extreme cases the user may pretend to be another user and infiltrate the system.

As noticed, the security requirements in distributed systems are totally different from the requirements in centralized (Client/Server) systems and therefore should be addressed differently too. (See in following Figure :)



The Distributed Security Approach

1.3 Application of the Layered Design in Data Security

Layered design (Clifford, 1998) is a technique whereby it is possible to dismantle complicated programs into a hierarchy of services. Each layer has a service interface defining the services the layer provides. It is possible to add stronger services by adding new layers over the layers rendering more basic services. The layered system also constitutes an excellent framework for explaining and organizing communication between two independent
Programs.

Communication between two programs may be dismantled into similar layers (identical) in each program.

The following three principles constitute the basis of the
Layered system:-

1.3.1- Each of the parallel layers on the server and the client together provides service. The protocol specifies how the work is divided, the format of the messages and the order of the transactions.

1.3.2- Each layer is built on the service of the layer under it. The service interface defines how each layer requests and receives the services of the layer under it. The interface must hide all the details of the work carried out under it and supply a full collection of services.

1.3.3- At the higher layers the service is simpler.

For example: the lower layers may use the system's services for hardware access on the computer while the higher layers render services such as Transfer of files etc.
We will apply the layered system in the design of the security system active portion in the client/server environment.

The server can store various kinds of data in large scopes, such as: documents, pictures, video, sound etc. The model of the layers of the security system divides the server and client programs into three layers: the application layer, the talk layer and the communication layer.

2. Computer Networks:

A **Computer Network**, often simply referred to as Network, is a collection of hardware components & computer Interconnected by communication channels that allow sharing of resources and information.

Networks may be classified according to a wide variety of characteristics as the medium used to transport the data, communication protocol used, Scale, topology, and organization scope.

2.1 TCP/IP(Transfer control protocol & Internet protocol)

TCP/IP is network protocol used on LANs, WANs and the Internet, but not everyone who uses it understands how it works. It's possible to use TCP/I P with little more than knowledge of how to configure the protocol stack, but a better understanding will give you a clearer picture of what is going on in your network and why the protocol needs to be set up in a particular way.

TCP/IP stands for Transmission Control Protocol/Internet Protocol. If this leads you to think that it is not just one protocol, you're right. In fact, it is not just two protocols, either. TCP/IP is a suite of protocols. We'll cover the most important ones in the course of this article.

"A router examines every packet, and
Compares the destination address with a
Table of addresses that it holds in memory."

2.1.1 Layered Protocol

Like most network protocols, TCP/IP is a layered protocol. Each layer builds upon the layer below it, adding new functionality. The lowest level protocol is concerned purely with the business of sending and receiving data - any data - using specific network hardware.

2.1.1.1 Link Layer

TCP/IP is a four-layer protocol, as illustrated in Figure 1.The lowest level, the link layer, is implemented within the network adapter and its device driver. Like all the TCP/IP protocols, it is defined by standards. The standards for generic Ethernet-type networks are defined by the IEEE 802 Committee: for example, IEEE 802.3 for Ethernet networks, or IEEE 802.5 for Token Ring networks.

2.1.1.2 Network Layer

The next layer up from the link layer is called the network layer. The most important protocol at this level is IP, the Internet Protocol. Its job is to send packets or data grams - a term which basically means "blocks of data" – from one point to another. It uses the link layer protocol to achieve this.

2.1.2 Internet Protocol

IP is the bedrock protocol of TCP/IP. Every message and every piece of data sent over any TCP/IP network is sent as an IP packet. IP's job is to enable data to be transmitted across and between networks.

Hence the name: inter-net protocol. In a small LAN, it adds little to what could be achieved if the network applications talked directly to Ethernet. If every computer is connected to the same Ethernet cable, every message could be sent directly to the destination computer.

Once you start connecting networks together, however, direct Ethernet

Communication becomes impractical.

2.2 Network Structure And Topology Information –

IP address allocation, assignment, and utilization; subnet information and layout; virtual local area network (e.g., VLAN) allocation and utilization; switch, router, server, or other network appliance interface names; and network addresses.

2.3 Network And System Configuration Information –

Authorization and authentication system types, methods, and configurations; Router and switch configurations and access-lists (ACL); firewall types; configurations and rules; Intrusion Detection System (i.e., IDS) types configuration and rules; network traffic monitoring and management procedures and methods (e.g. quality of service/guaranteed throughput level - Quos and "packet shaper" information); and network management system capacities, type and configuration, and Voice over IP (i.e., VoIP) activity logs. This applies to any other network "service" such as but not limited to: mail, news, Domain Name Servers (i.e., DNS), Dynamic Host Configuration Protocol (i.e., DHCP), Lightweight Directory Access Protocol (i.e., LDAP), Active Directory (i.e., AD), Remote Authentication Dial-In User Service (i.e., RADIUS) or Kerberos. All logs, logging methods and procedures, and transactional information produced by or for any of these or similar systems are specifically considered critical to the protection of the IT infrastructure.

2.4 The Language of Computer Networks

To better understand the area of computer networks, you should understand the basic broad categories of computer networks and data communications. For example, you should be able to define each of the following terms:

- Computer network
- Local area network
- Metropolitan area network
- Wide area network
- Personal area network
- Data communications

- Voice network
- Data network
- Telecommunications
- Network management

2.5 Computer Networks - Basic Configurations

Understand each of the following configurations. Examine the figure from the text or create your own example for each configuration. Describe how this configuration works in simple terms. Describe one or more applications that use each configuration:

- Terminal-to-mainframe
- Microcomputer-to-mainframe
- Microcomputer-to-local area network
- Microcomputer-to-internet
- Local area network-to- local area network
- Personal area network-to-workstation
- Local area network-to- metropolitan area network
- Local area network-to-wide area network
- Sensor-to-local area network
- Satellite and microwave
- Wireless telephone

2.6 Network Architecture Models

OSI Model and its 7 layers including the basic functions performed at each layer: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Even though the OSI model is not the actual model used to support the Internet, its understanding is necessary as many networks and products often refer to the OSI model for definition.

It is also important to learn the Internet Model (or DOD model or TCP/IP model) and its 4 layers: (Network) Interface, Network, Transport, and Application. The Internet model is the model used to support all activities on the Internet.

2.7 Logical and Physical Connections

To avoid future confusion, you must know the difference between a logical connection and a physical connection. Note that the only physical connection in a network is at the physical or interface layer.

2.8 Data and Signals

Information that is stored within computer systems and transferred over a computer network can be divided into two categories: data and signals. Data are entities that convey meaning within a computer or computer system. If you want to transfer this data from one point to another, either by using a physical wire or by using radio waves, the data has to be converted into a signal. Signals are the electric or electromagnetic encoding of data and are used to transmit data.

2.9 Converting Data into Signals

Like data, signals can be analogue or digital. Typically, digital signals convey digital data, and analogue signals convey analogue data. However, you can use analogue signals to convey digital data and digital signals to convey analogue data. The choice of using either analogue or digital signals often depends on the transmission equipment that is used and the environment in which the signals must travel. There are four combinations of data and signals: digital data transmitted using digital signals, digital data transmitted using analogue signals, analogue data transmitted using analogue signals, and analogue data transmitted using digital signals.

2.10 Spread Spectrum Technology

Using a spread spectrum transmission system, it is possible to transmit either analogue or digital data using an analogue signal. However, unlike other encoding and modulation techniques, only an intended receiver with the same type of transmission system can accept and decode the transmissions. The idea behind spread spectrum transmission is to bounce the signal around on seemingly random frequencies rather than transmit the signal on one fixed frequency. Anyone

trying to eavesdrop will not be able to listen because the transmission frequencies are constantly changing.

2.11 Data Codes

One of the most common forms of data transmitted between a sender and a receiver is textual data. This textual information is transmitted as a sequence of characters. To distinguish one character from another, each character is represented by a unique binary pattern of 1s and 0s. The set of all textual characters or symbols and their corresponding binary patterns is called a data code. Two important data codes are EBCDIC and ASCII.

2.12 Physical Medium

All communications media can be divided into two categories: physical or conducted media, such as wires, and radiated or wireless media, which use radio waves. Conducted media include twisted pair wire, coaxial cable, and fiber optic cable. In wireless transmission, various types of electromagnetic waves, such as radio waves, are used to transmit signals. This chapter examines seven basic groups of wireless media used for the transfer of data: terrestrial microwave transmissions, satellite transmissions, cellular radio systems, personal communication systems, pagers, infrared transmissions, and multichannel multipoint distribution service.

- **Fiber Optic Cable**

Fiber optic cable is a thin glass cable approximately a little thicker than a human hair surrounded by a plastic coating. A light source, called a photo diode, is placed at the transmitting end and quickly switched on and off. The light pulses travel down the glass cable and are detected by an optic sensor called a photo receptor on the receiving end. Fiber optic cable is capable of transmitting data at over 100 Gbps (that's 100 billion bits per second!) over several kilometers. In addition to having almost errorfree high data transmission rates, fiber optic cable has a number of other advantages over twisted pair and coaxial cable. Since fiber optic cable passes electrically nonconducting photons through a glass medium, it is immune to electromagnetic interference and virtually impossible to wiretap.

Wireless Media

All wireless systems employ radio waves at differing frequencies. The FCC strictly controls which frequencies are used for each particular type of service. The services covered in this section will include terrestrial microwave transmissions, satellite transmissions, cellular radio systems, personal communication systems, pagers, infrared transmissions, and multichannel multipoint distribution service Terrestrial microwave transmission systems transmit tightly focused beams of radio signals from one ground based microwave transmission antenna to another. Satellite microwave transmission systems are similar to terrestrial microwave systems except that the signal travels from a ground station on earth to a satellite and back to another ground station on earth, thus achieving much greater distances than line-of-sight transmission. Satellites orbit the earth from four possible ranges: low earth orbit (LEO), middle earth orbit (MEO), geosynchronous earth orbit (GEO), and highly elliptical earth orbit (HEO).

Two basic categories of mobile telephone systems currently exist: cellular telephone and personal communication systems (PCS). Cellular digital packet data (CDPD) technology supports a wireless connection for the transfer of computer data from a mobile location to the public telephone network and the Internet. Another wireless communication technology that has grown immensely in popularity within the last decade is the pager. Infrared transmission is a special form of radio transmission that uses a focused ray of light in the infrared frequency range.

When designing or updating a computer network, the selection of one type of media over another is an important issue. The principal factors you should consider in your decision include cost, speed, expandability, distance, environment, and security.

References:

- Amoroso, E. (1994), Fundamentals of Computer Security Technology, chap. 7, Prentice-Hall, Englewood Cliffs, NJ.
- Appleton, K., & Elain, L. (1997), Network Security: Is Your LAN Safe? DATAMATION, 39, pp. 45-49.