Data Security Management in Distributed Computer Systems

Adi Armoni
Tel-Aviv University, Israel
armonia@colman.ac.il

Abstract

This research deals with data security management in distributed and client/server computer systems, placing special emphasis on access security. The paper presents the subject of data security management 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, Burlesson 1998, Guynes 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 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 systems, security management, access security, layered design.

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 (Appelton, 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.

Distributed systems

The most important part of distributed systems is its joint data network which is the nerve center of the organization and tends to grow with the development of the organization and the development of technology.

Sometimes the network will connect a number of independent organizations with management and other servers to form the distributed system. For example, it is possible to describe an organizational network in a large organization with a large number of divisions and departments (Bellovin, 1997).

Paper Editor: Lech Janczewski

The increase of connections results in greater inter-dependency of the systems and constitutes an environment with many challenges for data security management (Herald, 1998; Guynes, 2000).

Client/Server systems

Traditional distributed systems enable users to use data and applications on distant networks without confining them to networks that they are directly connected to. In client/server systems the traditional functionality of the mainframe is divided into two:

- A user interface and a nucleus of one or more applications activated at the peripheral station defined as a "client".
- Management of the database and part of the application activated on another system defined as a "server".

Through this division each component in the network may carry out the work for which it is most suited. The two parts of the application are connected via special software enabling transfer of messages between the client and the server. Client/server applications are very flexible and allow users to access databases on various networks all via a graphic interface, which does not exist on mainframe systems (Neuman, 1998).

Data security management – general problems

Unfortunately, development of data security in distributed systems takes place simultaneously with the development of the network, as described above.

Development in stages may result in an increase of the sensitive points in the network security, as described hereunder (Sanders, 2000).

In some non automatic security subsystems, manual login mechanisms force users to type their user name and password. Not only does this make the system inefficient, it even exposes the data security mechanism, for the users often write down their password on paper next to their working station, for everyone to see (White, 1999).

Furthermore, most users do not make a habit of changing their passwords every so often and continue using the same password over and over again.

Security system components in distributed computer systems

Distributed computer systems pose four main security 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 (Pfleeger, 1997).
- Access control - Implemented via access matrices, access lists, capabilities list. These lists define access authorization to the computer resources for the user.

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 (Appelton, 1997; Guynes, 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

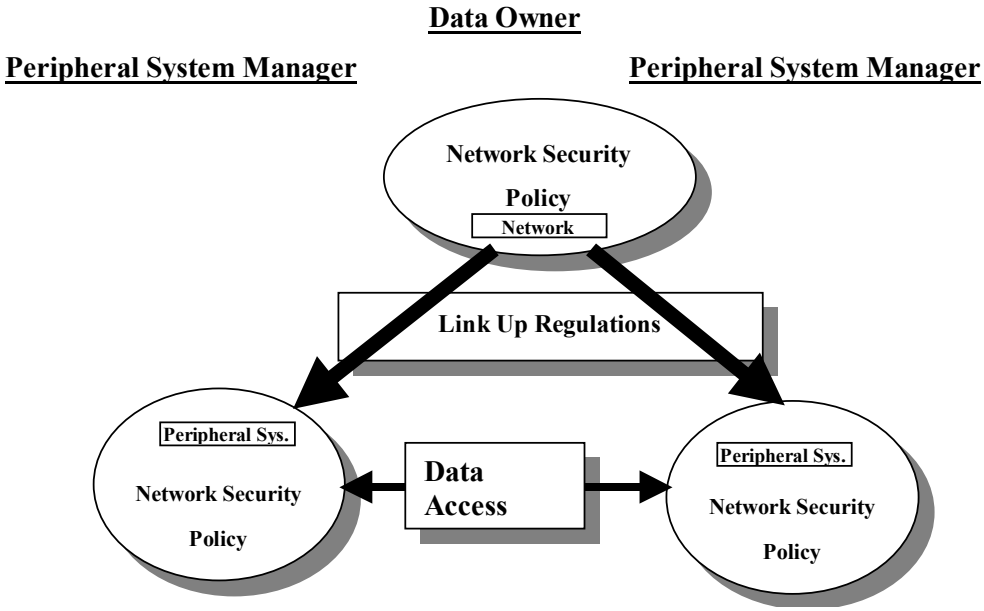

Figure 1 – The Distributed Security Approach

centralized (Client/Server) systems and therefore should be addressed differently too. (See Figure 1.)

Development of an Access Security System Model

In this part of the research we will present a model for an access security system operating in a local area network environment (LAN) with many stations and users. The model is for applications aiming at incorporating access security mechanisms in part of the applications which will render user sectionalizing services, supply passwords and authorization to users and stations of the network.

The model is mainly suitable for systems in which the operators use a large number of queries and transactions updating/cancellation/addition which must be sectionalized and classify users access. As an example we may use the data system at a bank branch. The system includes a large number of queries and bank transactions activated by clerks at the branch in accordance with the various departments. Sectionalization of the transactions and users at the branch may be according to the hierarchy at the branch: manager, deputy manager, department managers, clerks - or according to the nature of the departments: foreign currency, securities, current accounts etc. A clerk at the current accounts department will be able to carry out current account transactions only, while other transactions are blocked to him. The model we present here offers the full solution to these kinds of systems.

The model defines two main characteristics of access security: authority and authorization. Authority is the functionality level of the user in the organizational hierarchy. For example, at a bank branch the highest authority is the manager and then the department manager and so on.

The authorization sectionalizes the user's field of activity into fields that are specific to the organization. For example: there is authorization at a bank branch for foreign currency, current accounts, securities, etc.

As for the scope of the model, it encompasses the users of the work stations and the transactions they carry out.

Software architecture

The model is based on the Client/Server architecture as described in Figure 2. The access security server software may operate at each of the network stations as an independent application. The various applications (clients) will receive the access security services via an access security interface which must be incorporated in each application where these services are required.

The operational environment planned for the system is OS/2, but the model may be applied in other operational systems (WINDOWS 2000/NT) with minor changes. The communication mechanism between the interface software on the part of the client with the server software is NAMED PIPE.

A named pipe is a method for passing information from one computer process to other processes using a pipe or message holding place that is given a specific name. Unlike a regular pipe, a named pipe can be used by processes that do not have to share a common process origin

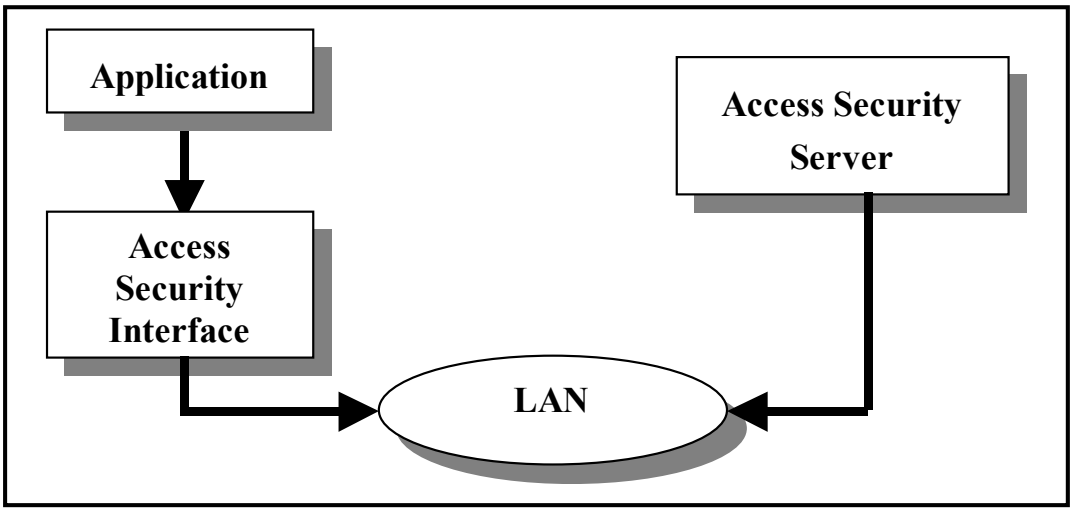

Figure 2 – Software architecture based on the Client/Server approach

and the message sent to the named pipe can be read by any authorized process that knows the name of the named pipe.

The most known feature of the named pipe is that it works using the "FIFO" method (first in, first out) i.e. the first data written to the pipe is the first data that is read from it.

Characteristics of Access Security in the System

The access security system refers to users carrying out a number of transactions at their work stations. For each transaction that may be carried out in the system a typical security label having two parts "security levels" and "security categories" is defined. Maximum authority is defined as well as the authorization/s granted to the station. For each user the maximum authority is defined as well as the authorization/s granted to him. (See Figure 3.)

Basic Rules

A number of basic rules must apply for the access security systems to function adequately. These basic rules vary but their core has been defined long ago and remains very much the same (Amoroso, 1994). Among them are rules such as:

- All users may operate from all stations, even if their maximum authority falls below the maximum authority granted to the station.
- In order to carry out a transaction at a station, the station must have authority that does not fall below the transaction authority, and the station must have the proper authorization (or more) for carrying out the transaction. Failure to meet one of the conditions will make it impossible to carry out a transaction.
- In order to carry out a transaction, the user must have authority that does not fall below the transaction authority, and also have the required authorization to carry out the transaction (or more than required). Failure to meet one of the conditions will make it impossible to carry out the transaction.

The services to be rendered by the system

The proposed access security system will provide a number of services for the client's applications which will enable a fair access security level. In addition to the server, there is of course back-up of each service and therefore the series of services mentioned hereunder applies both to the client and the service. The following are specifications of the access security services:

Employees

- Definition of a new employee
- Deletion of an existing employee
- Updating of employee's particulars for update/change
- Examination of the employee's validity
- Examination of employee's password

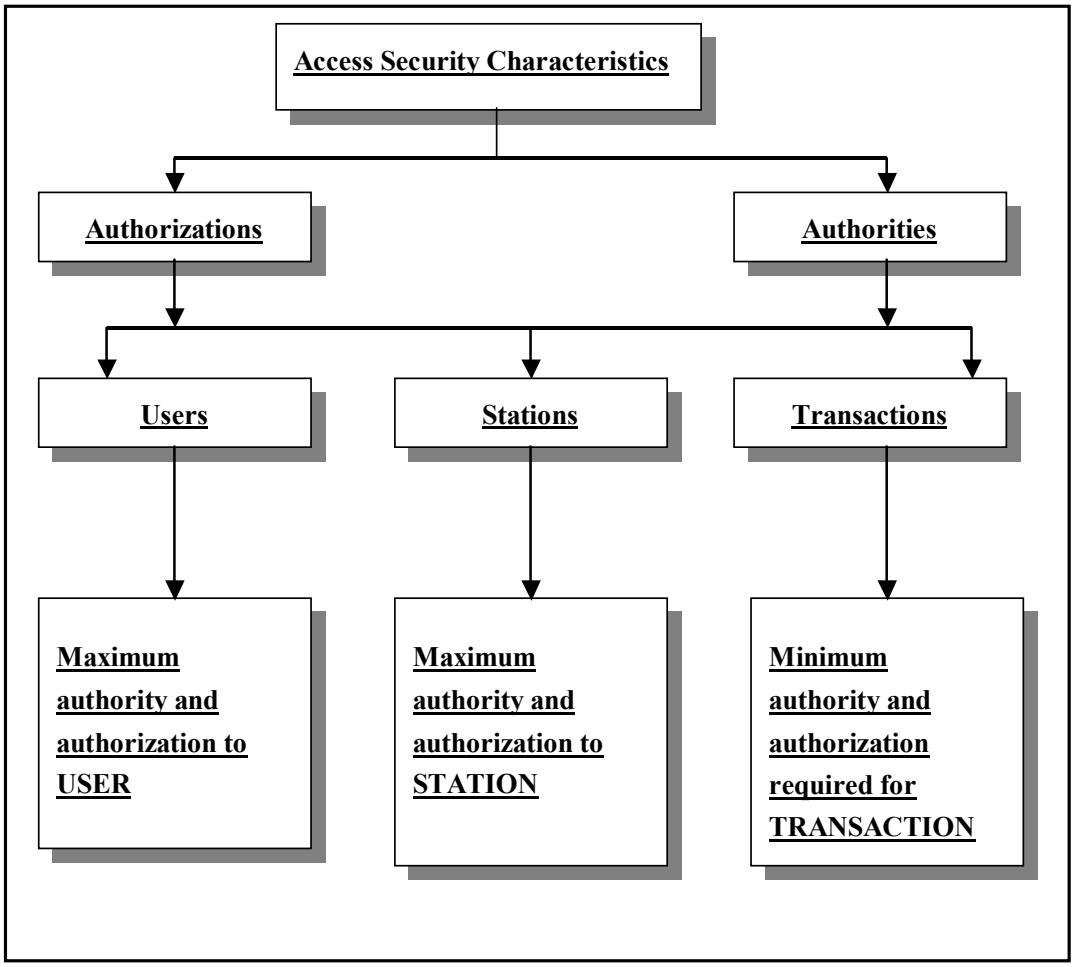

Figure 3 – Access security characteristics

- Receiving employee's authority
- Changing the password
- Setting free a blocked employee
- Receiving list of employee's authorizations

Stations

- Adding a new station
- Deletion of existing station
- Updating of the station's particulars

Transactions

- Definition of a new transaction
- Deletion of existing transaction
- Updating of the transaction details
- Receiving the list of transactions authority
- Receiving authority for transaction

Additional services

- Examination of a password's validity
- Primary password
- Registration of transactions in LOG
- Registration

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. Each of the parallel layers on the server and the client together provide service. The protocol

specifies how the work is divided, the format of the messages and the order of the transactions.
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.
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.

The application layer

On the part of the client, the application layer is the program requiring data security services, activating them through calling the service function in the high layer. Maintenance application of data security will supply employee definition services, object definition, granting authorization to employee/object, granting authority etc. On the server's part, the application layer carries out the client's request, approaches the files, checks the user's/application's authorization, carries out the examination of the password, change of password, employee definition, etc.

The talk layer

This layer provides the logic application of the access security. On the part of the server this layer analyzes the requests sent by the client, identifies the kind of service requested, prepares the proper parameters for carrying out the transaction, and returns to the application layer what is required to carry out the transaction.

On the part of the client, the layer constructs the message to the server so that it includes all the relevant data required. For example, in a request to check the user's password, this layer will prepare the identification particulars of the user, encrypt the password and add other details required on the part of the server. After the request is constructed these details will be passed on to the communication layer.

The communication layer

This layer carries out the actual transfer between the two processes. If the server and client are on the same computer, the communication takes place via Named Pipe IRC. If the client and the server are on different computers, the communication is carried out at one of the protocols of OS/2 based on LAN. The communication layer is applied as a generic layer that can use the named pipe, Netbios, TCP/IP and APPC/CPI. Realization of each of these systems may be applied separately, but their interface vis-à-vis the talk layer is identical, so that from the application's point of view, the protocol of data transfer over the LAN is transparent.

Architecture of the access security software

The access security server is composed from a number of layers and levels dealing with the various aspects of the software.

- *The communication layer*: Deals with communication vis-à-vis the clients, receiving messages and sending replies.
- *The talk layer*: Deals with identification and analysis of the messages received from clients, classifies the messages and separates them into the various parameters. This layer also constructs the client's reply transmission.
- *The application layer*: Operates on three main levels: handling requests for services regarding the user (definition, examination, deletion), handling requests for services regarding the station and handling requests for transaction services.

The services rendered comply with the requests the client may carry out, which were described in the talk layer on the client's side.

The application layer is assisted by an additional sub-layer of files services which supply all the transactions required for carrying out on the system's files, such as: search, update, cancel, ad, close etc.

Figure 4 is a schematic description of the software architecture of the access security server:

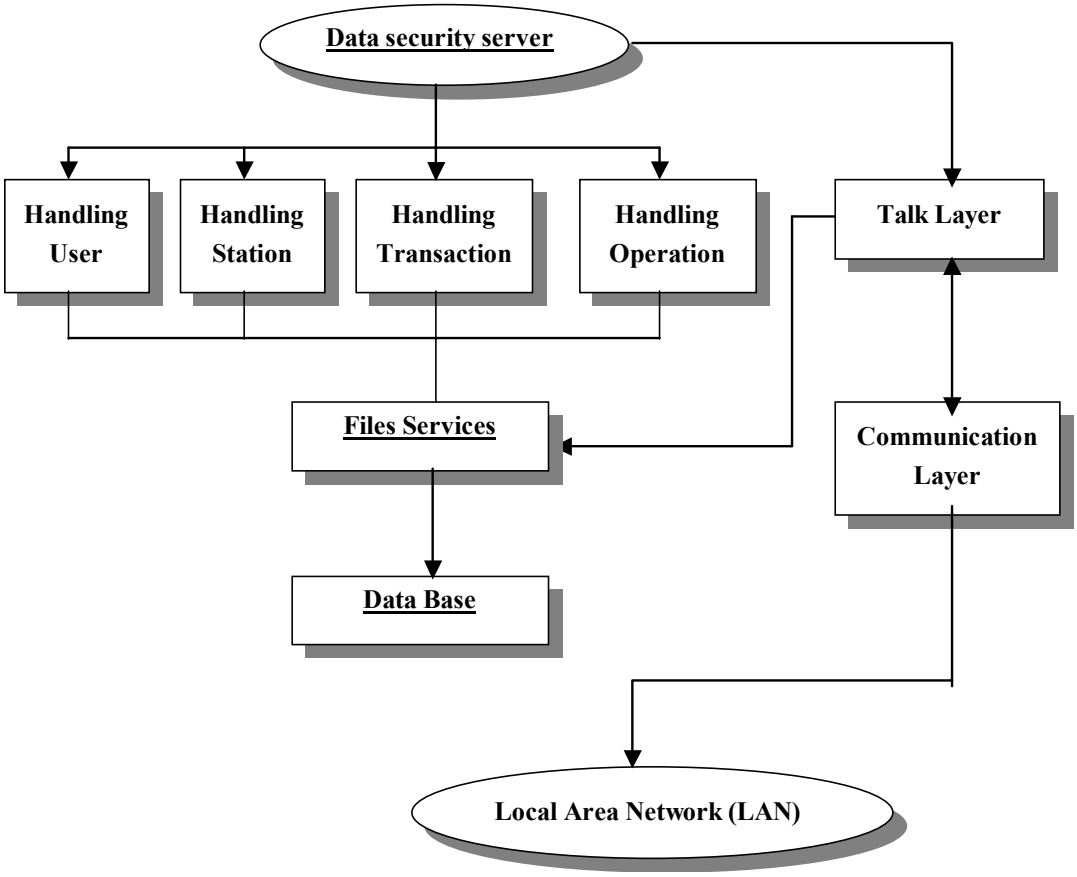

Figure 4 – Access Security Server – software architecture

Talk layer - Server's side

This layer analyzes the requests sent from the client, identifies the kind of service requested, examines whether the request is legal, ascertaining that the party making the request has the authority to make this particular request (whether the level of his/her authorization and authority and of the station from where he/she makes his/her request comply with the criteria of the request). Should this not be the case, this layer will send back a rejection message to the user. (See Figure 5.)

Furthermore, it prepares the parameters required for carrying out the request and returns the information required for carrying out the transaction to the application layer of the access security server. Once the request has been carried out by the access security application layer, the talk layer serves for the construction of the transmission to the client and the actual transmission of the message.

Application layer - server side

The application layer on the server carries out the access security server's transactions. The inputs to this layer are the client's various requests and the outputs of the layer are messages comprising the information requested by the client, or other information in case it is impossible to carry out the transaction.

Conclusion

The concerns many organizations have for protecting their data and applications from intruders in a large number of users environment, can be eliminated or at least attenuated. A new and innovative way to do so is through the implementation of an access security model.

The model developed in this research is a unique access security model with a client/server application. To date, the various models for data access security in a distributed system have not provided an effective and comprehensive solution dealing with all the aspects and levels of the computerized systems acting in the client/server environment. However, the model depicted in this article seems to answer all four security components of distributed computer systems: security authentication, authorization, access control and encryption.

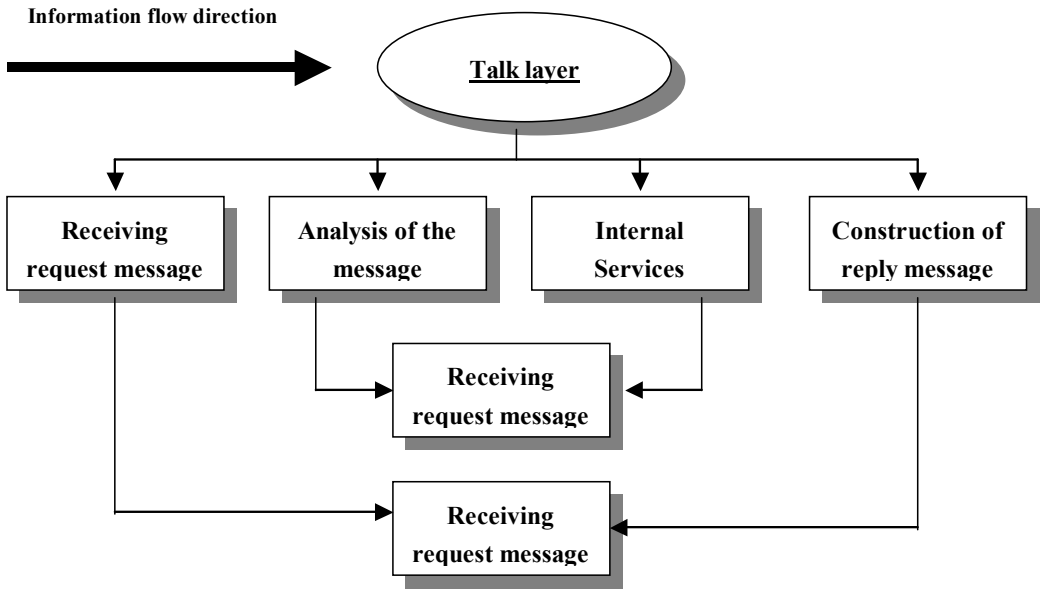

Figure 5 – Talk layer

To cater to the fact that security requirements of distributed systems are totally different from the requirements of centralized systems the proposed solution has been constructed using a unique anatomy of a program using a "Named Pipe", a security layered design and a robust 3 tier software architecture.

The variety of services rendered by this solution appeal now more than ever due to the increasing importance and the intensifying use of security management technology.

Managers of large local area networks with many stations and users who will implement the proposed model will surely reap the benefits using a variety of tools ranging from user sectionalizing services, supply passwords and authorization to users and stations of the network. From the above, it is apart that with these tools any organization or enterprise can lower the risk of unauthorized use and hostile takeovers of their vital data sources tremendously.

References

Amoroso, E. (1994), *Fundamentals of Computer Security Technology*, ch. 7, Prentice-Hall, Englewood Cliffs, NJ.

Appelton, K., & Elain, L. (1997), Network Security: Is Your LAN safe? *DATAMATION,* 39, pp. 45-49.

Bellovin, S., & Cheswick, W. (1997), Network Firewalls, *IEEE Communications Magazine*, pp. 65-70, September 1997.

Burleson, D. (1998), Managing security in a distributed database environment, *DBMS,* 8, pp. 72-77.

Clifford, R., Neuman, B., & Theodore Ts'o (1998), Kerberos: An Authentication Service For Computer Networks, *IEEE Communications Magazine*, September 1998

Elliot, P., *Pretty Good Privacy (PGP)*, Electronic Frontiers Houston, Internet (http://www.efh.org)

Guynes, C., Golladay R, & Huff R. (2000), Database security in a client/server environment, *SIGSAC Review,* 14, pp. 9-12.

Harold, J. H. (1998), Random Bits & Bytes, The Internet and Computer Security, *Computers & Security*, 13.

Neuman, D. (1998), Firewall Follow-Up, Data Communications, March 1998

O'Mahony, D. (1998), Security Considerations in a Network Management Environment, *IEEE Network*, May/June 1998

White, D. (1999), Distributed systems security, *DBMS,* 10, pp. 44-48.

Biography

ADI ARMONI, Ph.D. – Associate Dean and Head of computer and Information systems department, at the College of Management school of Business Administration, awarded Ph.D. degree in Information Systems from the school of Business Administration at Tel-Aviv University. Research subject deals with medical diagnosis from the artificial intelligence

point of view. B.Sc. in Industrial and Management Engineering

Dr. Armoni has published many articles in scientific journals and delivered lectures at international meetings and conferences. Dr. Armoni also serves as an associate editor for three leading journals in the field of Information systems and operation research. Major fields of interest in both research and practice are: Information systems policy, Health care information systems, E-commerce and decision support systems. Dr. Armoni is a senior consultant for the World Bank, and delivered many projects in Eastern Europe and South America. He serves as a senior consultant for many of the leading financial institutes, insurance companies, High-Tech firms and Health organizations in Israel, in the field of Computerized Information Systems Management.