MILITARY TECHNICAL COLLEGE
CAIRO - EGYPT

ICEENG 98

FIRST INTERNATIONAL CONF. ON
ELECTRICAL ENGINEERING

MULTILEVEL SECURITY IN LOCAL AREA NETWORKS: *ATRUSTED MODEL*

Dr. Eng M. Samy Gamal Eldeen **

Dr. Eng. Emad A. Fahmy *

Dr. Eng. Ismail A. Farag *

Dr. Eng Awad H. Khalil *

Cap. Eng. Ahmed AAbdel Hafez *

Abstract

This paper presents a new model that precisely describes the mechanisms that enforces the security policy and requirements for a multi-level secure Local Area Network. These mechanisms attempt to insure secure flow of information between entities assigned to different security classes in different computer systems connected to the network. The mechanisms also control the access to the network devices by the subject with different security clearances. Implementation of the security model has been shown during a complete discussion of the method of implementing the security requirements. The paper also gives an assessment of the proposed model compared to some commercial systems.

1- Introduction

The demand for protecting the privacy and the integrity of messages as they traverse the communication network has been on the increase in recent years. When a set of computers is introduced to form a network, the protection mechanisms residing within the individual computers inadequate to insure the security of interposes communications across the network. Such mechanisms can only prevent unauthorized access to the files and illegal flow of information between files stored within these computers become inadequate to insure the security of interposes communications across the network. This is due to the degree of openness of the network medium and the increased need for sharing resources within the network for accessing centralized storage facilities and for exchanging data and programs among users. Hence, security enforcement mechanisms for the network are required in addition to the existing protection mechanisms within the individual computers.

A network is said to be multilevel secured if it is able to protect multilevel information and users. That's, the information handled by the network can have different classifications and the network users may have varying clearance levels. Several approaches to network security have been proposed over the years that can be used to handle the problem of providing multi-level security in computer network.

2- Multilevel Security in LAN

The Local Area Networks' main philosophy is to have information and resources across distributed systems. This philosophy appears clearly from the definition of LAN which states that : "A Local Area Network (LAN) is primarily a data transmission system that aids the inter-communication between people or applications by the using of terminals or personal computers and their peripherals within the confines of restricted geographical area. "

From the previous definition of LAN we have seen that this philosophy is indirect conflict with basic security principles i.e., the control of access to information and resources. In other words, networking supplies general and flexible access while security imposes limited access using rigid control mechanisms.

A large number of security requirements for computer network has been identified in the literature. For purpose of this paper, we shall consider a subset of them to identify the basic requirements for a network to be secure as:

1-Control unauthorized access to the devices connected to the network i.e., the access to the network must be controlled by using a highly reliable user authentication mechanism.

2-Prevent the unauthorized dissemination of data stored in the network equipment.

3-Adequately protect the privacy and the confidentiality of data when transmitted on the communication channels.

4-The network must be able to record the occurrence of security relevant events in an audit log which known as accountability. This requirement is used only to adapt the security mode after operation.

Correspondingly, a secure network hence requires three types of control:

---

* *Staff Members of the Military Technical College*

1) Access control.

2) Cryptographic control.

3) Information flow control.

Recently, there are many studies have been focused on the security of computer networks. Some of the early work in this topic is reported in [1] which have attempted at a preliminary description of how multi-level security (i.e., protection of information of different security classification from users with different security clearances) can be provided in a computer networks. Protection against inter-process communication threats through the use of network protocols has been discussed by Voydock and Kent [2]. A more complete and conceptually more appealing development of security model for a specific application (Military systems) is given by GiLigan [3].

With the work on modeling security in stand-alone computer systems having attained a degree of maturity through the publication of the Trusted Computer System Evaluation Criteria (TCSEC) and its acceptance as a standard for the US Department of Defense (DOD) which published in 1985 and commonly known as Orange Book. It is natural to attempt to extend these concepts to network security problems. Anderson [4] and Walker [5] discuss initial arguments in this direction. Anderson [4] has proposed that network security issues can be handled with the same concepts that apply to the security of single computer systems and has presented the requirements for building a network that operates in the dedicated, system high, Controlled, and Multilevel modes (these four modes of operation are defined by the DOD in accrediting computer systems processing classified information and serve to categorize the degree of trust placed in them). Walker [5] has studied various ways of connecting both trusted and untrusted computer systems to a network in order to determine which portions of the overall network can be trusted and which security policy is to be enforced. Recently, STEVEN [6] has pointed the inadequacy of these studies in addressing some important security issues in distributed systems that may not be of particular relevance in stand-alone systems.

In order to briefly describe the additional complexities involved in designing a security mechanisms for computer network. Let us consider a typical Local Area Network that includes several computer systems that store data of various sensitivity levels. Several terminals that allow the users to access the network directly, several work stations between which data can be exchanged, several printers where the content of the files can be printed on a hard copy, and several other data bases, electronic mail servers etc., that can process data of different classification levels. Let us assume that the trusted systems are to process classified data. Such systems should have appropriate security mechanisms installed to support the control of information flow between the files and the users of the same system. In such an environment, when a piece of information that is classified at a certain sensitivity level in system is requested to be transferred to a file residing in different systems, or a network user wishes to access the network through a connected device, several additional problems should be taken into consideration. Firstly, due to the distribution nature of the network, any localized security enforcement mechanism (a reference monitor in the security kernel of a computer, for instance) cannot adequately mediate all access and protect all information transmitted over the network. Secondly, whereas the security enforcement mechanism for a computer system can be verified to control the information flow within the system, such a mechanism cannot enforce any security policy concerning the flow of information outside the system; i.e., the flow from one system to another system within the network. Furthermore, this mechanism cannot enforce the policy concerning the authorization of the access to the network devices by the network user or the process executed on behalf of the users. Hence, the problem of interest is how to design a security mechanism for a network which is trusted to process classified information at multiple security levels without comprising the security ? Evidently, implementation of a TCB in the processing elements

(Computer systems) attached to the network which performs access control functions alone will not be sufficient. A more elaborate security mechanism that is distributed across the network to perform both accesses control and information flow control functions is required.

In this paper, we shall describe a security model that precisely describes the mechanism enforcing the security policy for a network capable of handling information at different security classification levels and serving users with different security clearances. Figure 1 illustrates the physical configuration of this model, it comprises a physical secure communication network, to which both hosts and user terminals are connected via Trusted Interface Unit (TIU). The trusted network interface unit to ensure that the security policy is not violated mediates all communications across the network.

Host machines come in tow flavors: untrusted (uni-level secure) and trusted (multilevel secure). Untrusted hosts are considered uni-level secure to some specified level and all stored data are treated as if at that level. Trusted hosts are considered to be multi-level secure to some maximum level and contains data that may be associated with a level up to and including this maximum level. Users of the system are assumed to be trusted and are each assigned a security clearance level. Trusted Interface Unit (TIU) that connect users to the network consists of a Secure Terminal Server (STS) and a labeller / delabeller (ladel). The secure terminal server contains the virtual circuit security and management mechanism for the user end. Hosts are connected to the network via a Secure Host Server (SHS) and a (ladel). The SHS contains part of the virtual circuit management mechanism for the host end; the rest is in the host. The ladel is identical at both ends of the interconnection and enforce most of the system's security policy.

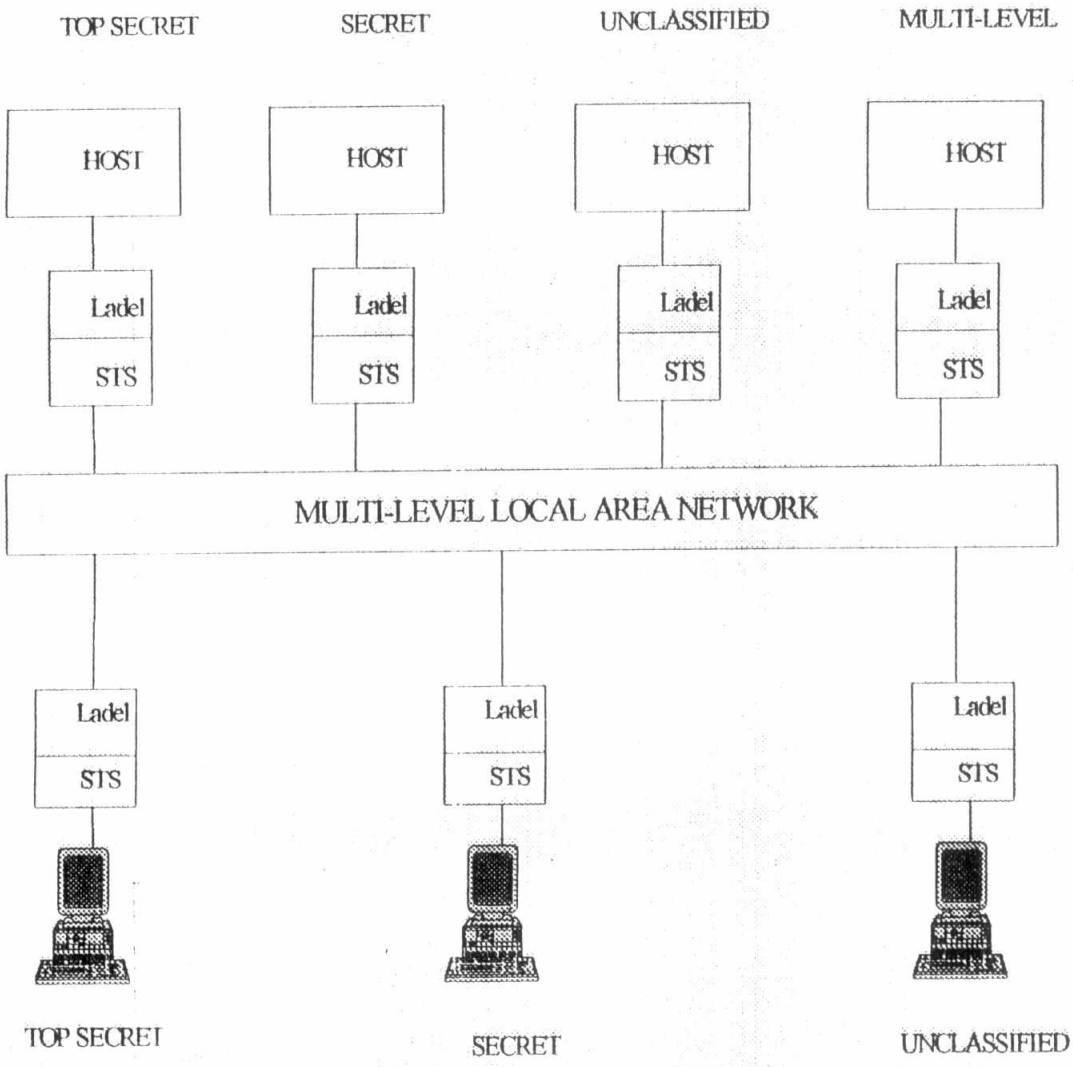

FIG.(1): Secured Network Model

Before designing the model the authors of the paper determine a number of requirements which must be verified through the implementation of the model, in which if these requirements are verified the security model will be a consistent one [7]. These requirements are:

1- Personal authentication (Access Control)

Using a highly reliable user authentication mechanism must control the access to the network (through a terminal or a host).

2- Labeling

Any information unit transmitted over the network (or stored in a memory location) must be labeled with its classification level.

3- Message flow

That of any recipient must dominate a message's security level.

4- Integrity

Each received message transmitted through the network must be unaltered, error free.

5- Confidentiality

A message transmitted through the network must be unintelligible to all users else the intended receiver.

6- Authenticity

Any message received must have been sent by a legitimate source.

7- Uniqueness

Any message received must not be a duplicate of a previously received message.

8- Order preserving

Message transmitted along a virtual circuit must be received in the order in which they transmitted.

9- Routing

A message is received only if the sender addressed it to the recipient.

10- Non-repudiation

Each message transmitted must be signed in such a way that it must be possible for the author of the signed message to subsequently disclaim the authorship.

11- Accountability

The network must not be able to record the occurrence of security relevant events in an audit-log.

3- Development of the formal model

In this section, the proposed model is described using some basic concepts of set theory to define the notion of a secure state and to describe the various operations and transformations that cause a change of state. It is known that the various operations and transformations are security preserving in the sense that a network stating from an initial secure state will only attain future states that are secure if the requirements stated in the previous section are satisfied [8].

Model description

Let SB denotes the set of all subjects included in the network,

U denotes the set of all network users, and

P denotes the set of processes executing on behalf of the users.

Clearly $U \subseteq SB$ and $P \subseteq SB$; also $U \cup P = SB$ and P and U are mutually exclusive i.e. $U \cap P = \emptyset$.

Let OB denote the set of all objects included in the network, and

OB consists of all data files, information units, physical memory location, and network devices ND, etc. Thus $ND \subseteq OB$

Let IO denotes that set of all I/O devices.

OT denotes the set of all output devices, and

PE denotes the set of all processing elements.

Evidently, $IO \subseteq ND$, $OT \subseteq ND$, $PE \subseteq ND$, $IO \cup OT \cup PE = ND$, and

$IO \cap PE = \emptyset$, $IO \cap OT = \emptyset$, $OT \cap PE = \emptyset$.

Instead of being restrictive in using the terms employed in military classification system such as "Top secret", "Secret", "Confidential", and "Unclassified" (this classification will be applied in the software program as a prototype [9]), the model will defines (for generalization) $SC = \{L_1, L_2, \ldots, L_n\}$ where n is a finite integer.

The relationship between two security classes within this set is denoted by $\leq$.

Let SI denote a set of subject IDs.

UI denote a set of user IDs, and

PI denote a set of process IDs,

Evidently, $UI \subseteq SI$, $PI \subseteq SI$, $UI \cup PI = SI$ and $UI \cap PI = \emptyset$.

Let RF denote a set of reference

In the following discussion, the corresponding lower case letters represent the elements of any set, for example. Then the Network Security Model (NSM) is defined by:

NSM = < S, S_o, OP, T>

Where:

S is a set of states

S_o is an initial state.

OP is a set of operations; and

T is a transformation function.

These quantities can be described as follows:

i) Set of states S

The states model are the state-dependent component in the secure network.

Each state s ∈S

S= (AT, SF, SL, SM, RM)

Where:

AT is the set of current access which is described by the triple (SB, ND, a)

SF is a security b nding function.

SL is the subject log in function.

SM is the subject mapping function.

RM is the reference mapping function

The current access triple AT= (SB, ND, a) is a set of current access that indicates which subject currently has the access to which network device. The existence or non-existence of access privilege is denoted by the access mode a, which has the representation {connect} for the existence of connect access privilege and a blank when connect access privilege does not exist. The access triple (SB, ND, a) may also be regarded as an access matrix whose rows represent the subject sb ∈SB and whose columns represent network devices nd ∈ND, and whose entry is the access mode (a).

The security binding function SF binds each entity to a security class sc ∈SC. It may be one of the three types of functions: clearance (CL). Current security level (CSL), and classification (CS). The clearance function CL: SB→SC binds each subject (user or process) to a security class.

Thus SC = CL (sb) represents the clearance of sb ∈SB. The current security level function CSL: SB → SC binds each subject sb to a security class representing the current level of sb such that CSL (sb) ∈ SC and CSL (sb) ≤ CL (sb). The classification function CS: OB → SC binds each object to a security class (or a range of security classes) i.e. CS (ob) = Sc represents the classification of ob ∈ OB.

The function subject-login, SL, is a one - to - one mapping from a subject of SI into RF, the set of references that correspond to network devices (i.e., a representation of processes and users being logged into specific network devices). Also, the function user-login, UL, is a one-to-one mapping form subset of UI into RF. Note That UI⊆ SI.

The function subject - mapping SM, is a one-to-one mapping from SI into SB. This function identifies a subject corresponding to subject ID. Also, the function user mapping, UM, is a one to one mapping form UI into U. Note that UI⊆ SI and U⊆ SB. The function reference mapping RM is a one-to-one mapping form a subset of RF into OB. This function identifies a specific object that is named by reference.

With the above definitions, it is possible to introduce the notation of state as follows:

A state is an element of S = (AT, SF, SC, SM, RM) where

AT is the access triple,

SF is the security binding function, which may be one of the three functions CL, CSL and CS,

SL is the subject mapping function, and

RM is the reference mapping function.

And they satisfy the following properties:

dom (CL) = rng (SM);

dom (CL) = rng (RM);

rng (CL) ∪ rng (CS) = SC

dom (CL) ⊆ dom (SM)

The initial sate S_o is a specific designated value attained by the state

ii) Set of operations OP

OP is a set of operations that affect the flow of information form one network device to another. These operations may change the security levels of the subjects and objects in the network. In the following, these operations will be introduced with a brief description of conditions (on the state variables) for executing the operation and the conditions that result from the execution.

1. The operation executed by subject sb ∈SB of transferring the contents of an object b ∈OB to another object d ∈OB is defined by TRANSFER (b,d), which represents the action that causes an information flow from object b to object d. The conditions for such transfer are CL(sb)≥ CS(b), and CS(b) ≤ CS(d). Note that the contents of the new d after the operation will be the concatenation of b and the old d, and this retains the classification CS(d).
2. The operation of creating a new file by a subject sb ∈SB With a classification SC is defined by CREATE (b,SC). The result of this operation is CS(b) = CSL (sb)=sc where sc ∈ SC.
3. The operation of changing the current security level of a user u∈U to a new level cl ∈ SC is defined by RECLASSIFY (U, CL). The security requirements for this operation are that cl = CSL (u) satisfy the conditions cl ≤ CL(U) and cl ≤ CS(Tu), whereTu ∈ ND is the terminal currently logged on by the user or a user with the role of Network Security Officer which is represented by NSO.
4. Finally, the operation of assigning a security class sc∈SC to an entity e∈SB ∪ ND is defined by ASSIGN (e,sc) which represents the action that uses the assignment of the security class sc (clearance or classification) to the entity (a subject or network device). This operation is restricted to be performed by a user with the role of NSO.

iii) Transformation function T

The transformation T describes the transition from one state to the succeeding state by applying one or a sequence of operations described above. It can hence be defined as a mapping T: SI X OP X S →S` where S` = T(Si,op,s) is the resulting state due to an operation op∈OP executed by a subject with ID si∈SI when the starting state is s∈S.

4- Implementation of the Security Model

To implement the security model, first, a studying of how to enforce the security requirements stated previously must be presented (this study is presented in [9]) showing the various mechanism to enforce each requirement and how to achieve the conditions for the network to be secure (fundamental to the concept of secure state are two properties , the set up security property and the connection security property) . Also the explanation of how these mechanisms will be embedded in the network layer was presented in [9]. Finally a prototype software system was developed in [9].

5- System Assessment

To evaluate the proposed model, a comparison with some commercial systems are presented in this section. These products have been evaluated by the NSA's Trusted Product Security Evaluation Division . The proposed model will be evaluated with the same manner.

VSLAN 5.0 (Verdix Secure Local Area Network)

-The highest class for which the VSLAN satisfies all the specified requirements of the TNI is class B2 MDIA network component

-The VSLAN satisfies the requirements for some of the security services described in part II of the TNI.

MLS LAN secure network server system

-The highest class at which MLS LAN secure network server system satisfies the requirements set in the TNI is A1 MI network component.

CX/SX with LAN /SX

-The highest class at which CX/SX with LAN /SX satisfies all the specified requirements of the criteria is class B1.

Trusted UNICOS 8.0

-The highest class at which the Trusted UNICOS 8.0 system satisfies all the specified requirements of the criteria class B1 MDIA network component.

Boeing

-The highest class for which the MSLAN satisfies all the specified requirements of the TNI is class A1 as an MDIA network component.

-The MSLAN provides some of the security services described in part II of the TNI (e.g. authentication, communication field integrity, and continuity of operations, network management, and selectivity routing.

Gemini Trusted Network Processor (GTNP)

-The highest class at which the GTNP satisfies all the specified requirements of the criteria as interpreted by the TNI is as an A1 mandatory-only network component.

The proposed model

-The highest class at which the proposed model satisfies all of the specified requirements of the TNI is A1 MDIA network component.

-The security policy supports both discretionary and mandatory access control (MAC) and (DAC).

-Auditing capabilities of the proposed model provide configurable options for recording security relevant events.

-The proposed model satisfies all the security services described in part II of the TNI.

A complete description of the previous systems can be found in [10].

6- Conclusion

The model introduced in this paper satisfies the eleven requirements that have been agreed upon in literature. The achievement of these eleven requirements will build consistent secure model to achieve a multilevel-secured Local Area Network.

The proposed model can be implemented in different ways, in different environment, so we consider that this model is a good field of research to achieve an optimum secure system.

REFRENCES

[1] M. DEVARGES "Local Area Network" 1992.

[2] VICTOR L. VOYDOCK. and STEPHAN T. KENT, "Security mechanisms in high-level network protocols "Computing surveys, vol. 15, No.2, June 1983.

[3] GILIGAN, J.M., and VASAK, J.M. "A generic security architecture for distribution systems" proceedings, seventh conference on Local Computer Networks. 1982

[4] PHILIP E. FITES, and ANDERSON "Information systems security: A practitioner' Reference "Van Nostrrand Reinhold 1993.

[5] STEPHEN T. WALKER "Network Security overview" IEEE Network Magazine 1995.

[6] STEVEN L. SHAFFER, and ALAM R. SIMON "Network security" academic press. inc. 1994.

[7] ANDREW J. MAZEIKIS, and GLENN H. MACEWEN "A communication protocol for A Multi-level Secure Network" IEEE Computer Magazine 1995.

[8] COLIN BOYD "Security Architectures using Formal Methods "IEEE Journal on selected areas in Communications vol. 11, No. 7 July 1985.

[9] A. ABDEL HAFEZ "Multi-level security for Local Area Networks" M.Sc. M.T.C. Cairo 1997.

[10] Trusted Product and Network Security Evaluation Division "The official list of products evaluated by the NSA's TPNSED www.mitre.org INTERNET 1996.