A Multi Upper Bound Access Control Model with Inheritance Attributes

Seok-Woo Kim

Abstract

A message server have two basic functionalities, a server role for processing the user environment as well as an entity role for transferring message to other entity in message system environment. The user who is going to send and receive his important information really wants to keep his own security requests. To satisfy this requirement, message server must be enforced by two seperated security policies - one for message processing security policy under department's computer working environment , the other for send/receive security policy under message system's communication path environment. Proposed access control model gurantees the user's security request by combining constrained server access control and message system access control with multi upper bound properties which come from inheritance attributes of originating user security contexts.

I. Introduction

Store and forward message systems that process classified information must operate in a secure manner, that is, they must adequately protects information against unauthorized disclosure, modification, withholding. one of the current research trend in computer and communication security is to faciliate the construction of multilevel secure system that protects information of multilevel secure if it can process and transfer in accordance with the intent of originator or sender as well as system security rules. Message system have two basic functionality-transferring the message from originating user to recipient through message server system, and processing message to being transferred to next message server or to provide service for user's request.

In other view point, message server have two working environment, one is the user environment where originate and recipient users are working under department security policy in local or remote domain, the other is the server environment where send/route/receive server are activating message transfer and process under message system security policy[1]. As the message have to be handled as an object a user agent at the same time as an entity in a message, message server must integrate the user and server's working environment, also the computing and communicating operations in a system. These dual natures of message system enforce the message server to operate as both an entity of message system and a server of end user. When we assume that the end user os working under high sensitive environment and the message server is working under secure message system environment, does the end user believe the message server? The message server must activate as trusted entity to service for user request, which means the sercret information can be flow down if the server is malicious.

The purpose of this paper is to provide access control model for message server to keep the sercet information fom unauthorized flow. To accompish these purpose, computer and communication security are intergrated to a message system, also constrained access control is enforced to message server. Computer security model has been reserched to describe the protection that a system actually provides and to define the security rules it is required to enforce. Traditional computer access control model has been started from BLP model[5], via integrated model[6], access control for trust server[8], unified access control model[10, 12], role based access control[13], For the message security, CCITT and ISO have recommended security service and architecture [1, 2, 3], and military message system[7]. All of these model and concepts describes one side of message system's point of view. This paper propose the actual access control property of message system which contain user security policies and message server system security policy, also contain consrained server access control policy and message system security as a single access control model enforcing multi security policies. These policies are consist of multi upper bound, ss, *, discretionary, marking, function control. The mub(multi upper bound) secure gurantees message system security by enforcing the user's security policy with inheritance property.

Manuscript received October 31, 1997; accepted November 29, 1997.

The Author is with Dept. of Information Communication, Hansei University, Goonpo, Kyounggi-do, Korea.

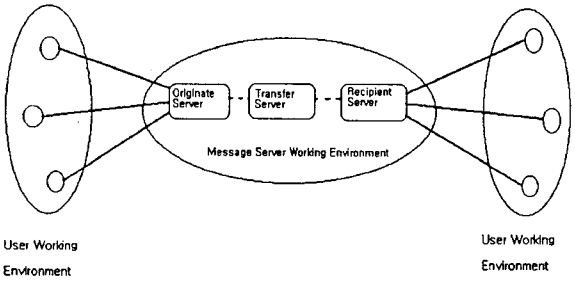

Fig. 1. Message system working environment.

II. Informal Description

Message system have two working environment, Department security policy is enforced to the message serve for processing the user's message-mandatory (ss, *), discretionary (ds), marking (mk) access control policy. Also every message server must be enforced by message security policy-authentication, encryption, integraty, security label which consist of mandatory and marking label.

In user working environment, user has an assigned maximum clearance level and category sets and user make a message to transfer to the desired recipient. This message have an access control list, job control list, the address of recipient, marking label.

Originating server activates in two role. As a department representive, originate server scrutinizes the user's message and checks the department policy of outgoing control. Also, as an entity of message server system where message server build a transfer message which contain the desired recipient server address, assigning the sensitivity and marking label relate to message server system security policy. As the result, message have dual security policy labels come out from user security policy and message security policy. The transfer messager server have to do three actions. (1) A communication security is needed to connect next transfer message server which is in the path of from originating to recipient server. (2) After receiving the transfer message, message server access the received message for transfer and services. (3) These access must be enforced by proposed model resulting in secure process and transfer and keep the user's security policy. The recipient message server acts same to origiante server but reverse process.

1. Security Requirement

In this model, we can say that system is secure if the user is enforced by security policy which keep the multi upper bound property. This property protects the user's message from unauthorized information flow by following operating environment.

(A1) There exist a message system security officer and department security officer for any department environment. Since officer assigns right security attributes to the subject

(A2) Every subject works within his maximum assigned security attributes.

(A3) Every object also have security attributes

(A4) Communication channel has a single mandatory label

(A5) There exist reliable message transfer protocol and message should be received by intended recipient

(A6) Security Attributes of each department are either comparable or not. It depends on department's policy

(A7) Each system have it's own security policy which are come from a multi access control policy

III. A Multi Upper Bound Access Control Model

In this section we define the 4 operators and state dependent components in multi upper bound(mub) access control model. After then, present a formal access control model and verification of the mub and ss properties. Others can be verified in same manner.

1. Operators

The major 4 operations are defined as the below followings - dominate operator $\geq$, mandatory access control label upper bound operator $\otimes$. message address upper bound operator $\otimes$, marking label upper bound operator $\oplus$

$\geq$ represents dominate relation of mandatory access label *macl*. Mandatory access label *macl* is consist of identifier *id*, sensitivity level *sl*, category $\{cat_1, cat_2, \ldots\}$. $sl_1 \geq sl_2$ means sl_1 dominates sl_2, $cat_1 \geq cat_2$ means cat_2 is set of cat_1.

$\otimes$ is upper bound property operator of *macls*. For example, if there exist 3 *macls*, $macl_1 = (id_1, sl_1, cat_1)$, $macl_2 = (id_2, sl_2, cat_2)$, $macl_3 = (id_3, sl_3, cat_3)$, and $sl_2 \geq sl_2$, $cat_2 \geq cat_3$, then $macl_2 \otimes macl_3 = (id_2, sl_2, cat_3)$ and $macl_1 \otimes macl_3 = (id_1, sl_1, cat_1), (id_2, sl_1, cat_2)$

$\odot$ is upper bound property operator of recipient address. If *sdacl* represents recipient address-servers discretionary access label and $sdacl_1 = \{svr_1, svr_2\}$, $sdach_2 = \{svr_1, svr_3\}$, $sdacl_3 = \{svr_4, svr_5\}$ exist then, $sdacl_1 \otimes sdacl_2 = \{svr_1\}$ and $sdacl_1 \otimes sdacl_2 = \emptyset$

$\oplus$ represents upper bound property of operator of marking label. If *mkcl* represents marking label and $mkcl_1 = \{(id_1, \{mark_{11}, mark_{12}\}), (id_2, \{mark_{21}, mark_{22}\})\}$, $mkcl_2 = \{(id_1, \{mark_{11}, mark_{13}\})\}$ exist, then $mkcl_1 \oplus mkcl_2 = \{(id_1, \{mark_{11}, mark_{12}, mark_{13}\}), (id_2, \{mark_{21}, mark_{22}\})\}$.

2. Model Components

We assume that the following sets are exist.

S set of subjects. $S = USR \cup SVR$.

O message content which is object to be protected.

Sid set of subject identification. $Sid = USRid \cup SVRid$.

Oid set of object identification.

SL $SL \subseteq SMACL \times SDACL \times SMKCL \times JCL \times UMACL \times UDACL \times UMKCL$.

$SMACL \subseteq LEV \times CAT$, LEV is a set of security level, CAT is a set of categories.

$UMACL \subseteq Did \times LEV \times CAT$, Did is a set of deparart-ment id.

$UDACL \subseteq S \times A$, $A=\{r,w\}$

$SDACL \subseteq Sid$,

$UMKCL \subseteq Did \times MKCL, MKCL$ is a set of marking.

JCL is a set of well formed function names.

SF Sunction from Sid to S.

OF Function from Oid to O.

AX Current access set of system.

LF Security binding function.

$PRIVF$ Function from S to P^2. P is a set of privieges.

CM a set of connect permission matrix. CM_{kk} is a matrix, $CM_{ij} = \{c_o, c_i\}$ means i'th subject permit connect-in and connect-out to j'th subject.

3. A Multi Upper Bound Access Control Model

Definition 1 : A *system state st* is an element of $(SF, OF, AX, PRIVF, CM)$

$SF : Sid \rightarrow S$

$OF : Oid \rightarrow O$

$AX \subseteq SO \times UO \times SS \times SSO$

$SO \subseteq SVR \times O \times (A \cup P \cup J)^2$

$UO \subseteq USR \times O \times (A \cup P)^2$

$SS \subseteq S \times S \times (C \cup P)^2$

$SSO \subseteq S \times S \times O \times (T \cup P)^2$

LF:

$SMAC : SVR \rightarrow SMACL$, $UMAC: USR \rightarrow UMACL$

$SMKC : SVR \rightarrow SMKCL$, $UMAC: USR \rightarrow UMACL$

$CSMAC : SVR \rightarrow SMACL$

$CSMKC : SVR \rightarrow SMACL$

$CDAC : SVR \rightarrow SVR \times SDACL$

$CJCL : SVR \rightarrow SDACL$

$OSSL : O \rightarrow SMACL \times SMKCL \times SDACL$

$OUSL : O \rightarrow UMACL \times UMKCL$

$OJCL : O \rightarrow JCL^2$

$OACL : O \rightarrow UDACL$

$BL : O \rightarrow S \times S \rightarrow SMACL$

$PRIVF : S \rightarrow P^2$

$CM = \{CM_{11}, CM_{22}, CM_{33} \ldots CM_{KK}\}$

Definition 2 : A system $\sum$ is a 4 tuple $(I, ST.st_0, TR)$, where I set of system repuests.

$i \in I = (SVR \times O \times (A \cup P \cup J)) \vee (USR \times O \times (A \cup P)) \vee (S \times S \times (C \cup P)) \vee (S \times S \times O \times (T \cup P))$;

ST is the set of possible system states;

TR is the system transform function: $S \times I \times ST \rightarrow ST$

Definition 3 : A *history* is a function from a set of non-negative integers N to $S \times I \times ST$ such that(1) the third element of $\Pi(0)$ is st_0, and (2) $\Pi(n) = (s,i,st) \wedge \Pi(n+1) = (s', I', st') \Rightarrow TR(s, I, st) = s'$

Definition 4 : A state st is *multi upper bound(mub) secure*

if$(svr_i, o_j, r) \in$ so, then

$[CSMAC(svr_i) \geq OSMAC(o_j)] \wedge [CUMAC(svr_i) \geq OUMAC(o_j)] \wedge$
$[CSMAC(svr_i) \geq OSMAC(o_j)] \wedge [CUDAC(svr_i) \subseteq OUDAC(o_j)] \wedge$
$[CSMKC(svr_i) \supseteq OSMKC(o_j)] \wedge [CUMKC(svr_i) \supseteq OUMKC(o_j)] \wedge$
$[CSJCL(svr_i) \subseteq OSJCL(o_j)]$

if$(svr_i, o_j, w) \in so$, then

$[CSMAC(svr_i) \ll OSMAC(o_j)] \wedge [CUMAC(svr_i) \ll OUMAC(o_j)] \wedge$
$[CSDAC(svr_i) \supseteq OSDAC(o_j)] \wedge [CUDAC(svr_i) \subseteq OUDAC(o_j)] \wedge$
$[CSMKC(svr_i) \subseteq OSMKC(o_j)] \wedge [CUMKC(svr_i) \subseteq OUMKC(o_j)] \wedge$
$[CSJCL(svr_i) \supseteq OSJCL(o_j)]$

Definition 5 : A state st is *ss secure*

if$(usr_i, o_j, r) \vee (usr_i, o_j, w) \in uo$, *then* $UMAC(usr_i) \geq OUMAC(o_j)$

if$(svr_x, svr_y, c_i) \vee (svr_x, svr_y, c0) \in ss$,

than $SMAC(svr_x) \geq BL(svr_x, svr_y)$

Definition 6 : A state st is * *secure*

if$(usr_i, o_j, r) \in uo$, *then* $CUMAC(usr_i) \geq OUMAC(o_j)$

if$(usr_i, o_j, w) \in uo$ *then* $CUMAC(usr_i) = OUMAC(o_j)$

if$(svr_x, svr_y, o_z, t) \vee (svr_x, svr_y, o_z, rx) \in sso$ *the* $OSMA(o_z) = (svr_x, svr_y)$

Definition 7 : A state st is *ds secure*

if$(usr_i, o_j, r) \vee (usr_i, o_j, w) \in uo$, *then* $r \vee w \in OACL\ (o_j)$

if$(svr_x, o_m, ci) \vee (svr_x, svr_y, c_0) \in sso$, *then* $c_i \vee c_o \in CM_{xy}$

Definition 8 : A state st is *marking secure*

if$(usr_i, o_j, r) \in uo$, *then* $SMKC(usr_i) \supseteq OUMKC(o_j)$

if$(svr_x, svr_y, o_z, rx) \in sso$ $SMKC(svr_y) \supseteq OSMKC(o_z)$

IV. Verification of a Secure System

A system state is a picture of at any time in system behaviour, if all the state of system is secure, then we can say system is secure.

In this section, a secure system state is verified if that state is transformed from previous state keeping multi upper bound, ss, *, ds, marking, privilege security property as definition 4.

(theorem1) st' is mub secure if st is *mub secure* and (svr_i, o_j, a) exists at new stste st' and keeps the following conditions.

(1) a = r

$[CSMAC(svr_i)=CSMAC(svr_i)\otimes OSMAC(o_j)]\wedge$
$[CUMAC(svr_i)=CUMAC(svr_i)\otimes OUMAC(o_j)]\wedge$
$[CSDAC(svr_i)=CSDAC(svr_i)\odot OSDAC(o_j)]\wedge$
$[CUDAC(svr_i)=CUDAC(svr_i)\odot OUDAC(o_j)]\wedge$
$[CSMKC(svr_i)=CSMKC(svr_i)\oplus OSMKC(o_j)]\wedge$
$[CUMKC(svr_i)=CUMKC(svr_i)\oplus OUMKC(o_j)]\wedge$
$[CSJCL(svr_i)= CSJCL(svr_i)\odot OSJCL(o_j)]$

(2) a = w
$[CSMAC(svr_i)\leq OSMAC(o_j)]\wedge[CUMAC(svr_i)\leq OUMAC(o_j)]\wedge$
$[CSDAC(svr_i)\supseteq OSDAC(o_j)]\wedge[CUDAC(svr_i)\subseteq OUDAC(o_j)]\wedge$
$[OSMKC(o_j)]=OSMKC(o_j)\oplus CSMKC(svr_i)]\wedge$
$[OUMKC(o_j)=OUMKC(o_j)\oplus CUMKC(svr_i)]\wedge$
$[CSJCL(svr_i)\supseteq OSJCL(o_j)]$

(Verification)

($\Leftarrow$) if *st'* satifies mub property,(1),(2) is satisfied by definition 4

($\Rightarrow$) As *st* satisfies mub property and (svr_i,o_j,a) in state *st'* has the (1),(2) conditions , for the ax'-ax = (svr_i,o_j,a)

(1) a= r , then
$[CSMAC(svr_i)\otimes OSMAC(o_j)\geq OSMAC(o_j)]\wedge$
$[CUMAC(svr_i)\otimes OUMAC(o_j)\geq OUMAC(o_j)]\wedge$
$[CSDAC(svr_i)\odot OSDAC(o_j)\subseteq OSDAC(o_j)]\wedge$
$[CUDAC(svr_i)\odot OUDAC(o_j)\subseteq OUDAC(o_j)]\wedge$
$[CSMKC(svr_i)\oplus OSMKC(o_j)\subseteq OSMKC(o_j)]\wedge$
$[CUMKC(svr_i)\oplus OUMKC(o_j)\subseteq OUMKC(o_j)]\wedge$
$[CSJCL(svr_i)\odot OSJCL(o_j)\supseteq OSJCL(o_j)]$

(2) a = w, then mub property condition exists. *st'* which contains new creating (svr_i, svr_j,a). satisfing the mub property.

(theorem2) System state *st* satisfies the ss property, if (usr_i, o_j, a) and (svr_x, svr_y, c) in *st'* which is not exist in previous state *st* exist in state *st'* and satisfy the following conditions;

(1) a = r $\vee$ a = w, then $SMAC(usr_1)\geq OUMAC(o_j)$
(2) c = c_i $\vee$ c = c_0 , then $SMACLF(svr_x)\geq BL(svr_y)$

(Verification)

($\Leftarrow$) If *st'* satisfies the ss property, (1), (2) is satisfied by definition 5.

($\Rightarrow$) AS *st* satisfies the ss propert and new creating (usr_1, o_j, a), (svr_x, svr_y, c) have (1) and (2) conditions.

(1) ax $\cap$ ax* keeps ss property

(2) ax* - ax = (usr_i, o_j, a), (svr_x, svr_y, c) have the ss property condition the new creating (usr_i, o_j, a)(svr_x, svr_y, c) in st' satisfies ss property condition the other properties - *, ds, marking, privilege, properties are verified like the above manner.

V. Conclusions

In this paper. we models the secure message server which enforcing multi upper bound property. The message server activates as three entities - depatrment security manager, member of message server system, and server for user request. As a result, message server must be enforced by three security policies. Especialluy in case of activates as a server for user request, it must keep user's security policy which consist of mub policies. Model assumes that the security policy of user and server are combined with computer security model and traditional message system securityservice. This combined security policy can enforce the message server's access when it activates as a controlled entity, but another security policy is needed when it activates as a service provider. Because the intrinsic functionalitty of message system is so complicated, it is very difficult to apply any existing model without modification.. This paper proposes the unified and expanded access control model for secure message server. Model represents just atomic access of message system. it needs more refined definition. and operation for real application.

References

[1] CCITT, *Data communication Networks Message Handling Systems*, Recommendations X.400 - X.420, Nov. 1988.

[2] ISO/IEC, *Information Processing System - Open Systems Interconnectionn - Basic Reference Model - Part 2* : Security Architecture, Feb. 1989.

[3] ISO/IEC, *Information Technology - Open Systems Inercon-nection - Security Frameworks in Open Systems - Part3* : Access Control, Jun. 1992.

[4] Department of Defence Computer Security Center, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria,* NCSC-TG-oo5, Version 1, Jul. 1987.

[5] D. E. Bell, L. J. LaPadula, *Secure Computer Systems : Unified Exposition and Multics Interpretation,* Technical Report ESD-TR-75-306, The MITRE Corporation. Bedford, MA, 1976.

[6] K. J. Biba, *Inergrity Consideration for Secure Computer Systems,* Technical Report ESD-TR-76-372, The MITRE Corporation, Bedford, MA, 1976.

[7] J. Landwehr, C. Heitmeyer, and J. McLean, "A Security Model for Military Message Systems," *ACM Trans. on Computer Systems,* Vol. 2, No. 3, pp. 198-222, Aug. 1984.

[8] J. Landauer, T. Redmond, and T. Benzel, "Formal Policies for Trusted *Processes," Proceeding of the Computer Security Foundation Workshop III.* pp. 31-40, Jun. 1989.

[9] E. Bertinto, Sanmarati P., Jajodia S., "High Assurance Discretionary Access Control for Object Bases," *Proceeding of the first Conference on Computer and Communication*

Security, Fairfax, VA, ACM SIGSAC, pp. 144-150, Nov, 1993.

[10] L. J. LaPadula, "Formal Modeling in a Generalized Framework for Access Control," *Proceeding of the Computer Security Foundation Workshop III,* pp, 100-109, Jun. 1990.

[11] J. P. L. Woodward, "Exploting the Deal Nature of Sensitivity Labels, *"Proceeding of the 1987 Symposium on Secu rity and Privacy,* Oakland, CA, IEEE Computer Society Press, pp. 23-30, Apr. 1987.

[12] M. D. Abrams, K. W. Eggers, and L. J. LaPadula, "A Generalized Framework for Access Control : An Informal Description," *Proceeding of the 13th National Computer Security Conference,* Baltimore, MD, pp. 135-143, Oct. 1989.

[13] D. Ferrario, R. Kahn, "Role-Based Access Control Models", *Proceeding of the 15th National Computer Security Conference,* Gaithersberg, MD., pp.554-563, Oct. 1992.

Seok-Woo Kim received the B.S. degree in Communication Engineering from Hankook Aviation College, Goyang, Kyonggi-do, Korea in 1979. He received the M.S. in Computer Information Science from New Jersey Institute Technology of NJ, USA in 1989, and Ph.D. degree in Computer Engineering from Ajou University in 1995. He is currently an assistant professor in the Department of Information Communication at Hansei University, Goonpo, Kyounggi since 1997. He has been researched and developmented in ETRI from 1980 to 1997 in the field of information security, also in Bell Lab. from 1987 to 1989. He is the chief member of open security architecture research group in KHSC, also a member of editorial board of JEEIS, KHSC, KIPS, a member of TTA ISO/ IEC SC10, ECMA TC68. His current research interests in the open security architecture and its application.