通信情報保護學會論文誌
第4卷 第2號, 1994. 12

두개의 다중 보안정책을 준수하는 메세지서버 액세스 제어 알고리즘

김 석 우*, 김 동 규**

The Message Server Access Control Algorithm Enforcing Two Multi Security Policies

Seok Woo Kim and Dong Kyoo Kim

요 약

메세지 전달시스템을 이용한 원거리 정보전달이 일반화되고 있다. X.400 메세지 처리시스템 및 OSI 보안구조는 보안기능 및 서비스에 대한 표준을 개념적으로 정의하고 있으나, 메세지 전달시스템이 제공하는 보안서비스에 의존하여 중요정보를 송·수신하는 유저는 자신의 보안정책이 준수되기를 원한다. 이를 위해, 메세지 전달시스템과 유저의 독립적 또는 중첩된 2개의 다중 보안정책이 메세지 서버에서 준수되어야 한다. 메세지의 전송 및 프로세싱은 주체와 객체가 지닌 보안레이블이 강제적, 임의적, 마킹, 특권제어의 다중 보안정책에 부합될 때 액세스가 허용된다. 제안된 알고리즘이 메세지 서버에서 보안메카니즘으로 동작될 때, OSI 보안구조와 유저가 요구하는 보안요구조건이 만족됨으로써, 유저의 메세지가 안전하게 전송될 수 있다.

Abstract

By using message transfer system, remote information transfer is becoming generalized. Even the X.400 message handling system and OSI security framework conceptually define security function and service standards, the user who is sending and receiving his important information by using the provided security services of message transfer system really want to keep his own security policy. To do so, seperate or unified 2 security policies of message transfer system and user are to be enforced on the message server. The message transfer or processing is permitted when the security label of subject and that of object are compatible to these multi security policies of mandatory, discretionary, marking,

* 한국전자통신 연구소
** 아주대학교 컴퓨터 공학과 교수

privilege control. When the proposed algorithm is activated as a security mechanism in the message server, security requirements of user and OSI security architecture are satisfied, resulting in the secure transfer of user message.

1. 서 론

최근들어 메세지에 의한 정보전달이 보편화되면서 표준화된 메세지 처리시스템(MHS)이 CCITT X.400[1]으로 권고되었다. MHS의 전달 및 서비스 기능을 이용하여 정보 전달을 원하는 유저입장에서 보는 MHS는 신뢰할 수 있어야 하며[23,24], 이를 위한 CCITT와 ISO의 보안 연구가 현재까지 진행 중에 있다[1,2,3,4]. 그러나, CCITT 및 ISO의 보안 연구는 엔티티와 엔티티 사이의 보안 서비스 및 보안 구조에 관한 것으로써 유저 입장에서 요구하는 유저 보안정책과는 별도의 관점에서 연구되고 있다. 유저 환경에서의 보안 요구는 주체가 객체정보를 액세스할 때, 주어진 보안정책에 부합되는가를 판단하는 컴퓨터 액세스 제어 모델에 근간을 두고 있다. 전형적인 컴퓨터 액세스 제어 모델 연구는 BLP 모델[5,6]에서부터 시작되어 무결성 제어 모델[7,8], 액세스 권한 제어 모델[12,13]을 거쳐 분산 환경의 종합 모델[15,17]로 발전되어 왔다. 컴퓨터 내부의 프로세서와 화일에 대한 일반적인 액세스외에 서버 프로세스에 대한 모델[11], 서버의 우회기능을 포함한 메세지 액세스 모델[10], 시스템 구현 관점에서 기준[6] 등이 계속적으로 연구되어 왔다. 본 논문은 메세지 처리시스템의 전달시스템 엔티티가 시스템의 구성 요소일 뿐만 아니라 유저 엔티티로서도 동작함으로써, 유저환경에서 요구하는 보안정책을 동시에 만족할 수 있다는 점에 착안하여, 최근까지 이슈화되고 있는 강제적, 임의적, 마킹[18,19], 특권 제어[13,20]를 유저와 전달시스템의 보안 정책으로 가정하여, 서버엔티티의 전송 및 프로세싱을 참조 모니터하는 액세스 제어 알고리즘을 제안한다. 알고리즘은 CCITT 및 ISO의 개념적 보안 서비스와 기능을 전달 시스템의 보안 레이블을 통해 전송 제어하며, 서버 프로세싱을 전달 시스템 및 유저 보안 레이블에 의해 원시 액세스 제어하는 보안 규칙들로 구성된다. 논문의 구성은 다음과 같다. 제2장에서는 보안레이블과 인터페이스를 포함한 메세지 처리시스템을 개념적으로 모델링하고, 제3장에서 액세스 제어의 근간이 되는 보안레이블 및 안전한 메세지 전송 및 프로세싱을 위한 정보흐름 제어 조건을 설명한다. 제4장에서는 이와같은 정보흐름 제어 조건을 메세지 서버에서 참조 모니터하는 알고리즘을 기술한다. 제5장에서 관련 연구와 비교·분석 후, 제6장에서 결론을 맺는다.

2. 메세지 처리시스템 모델

메세지 처리시스템은 메세지를 전달하고 전달된 메세지를 서비스하는 서버엔티티들과 메세지 전달을 의뢰하고 최종적으로 메세지를 수신하는 유저엔티티들의 집합으로 구성된다. 각 엔티티들은 유일한 이름을 지니며, 엔티티들의 특성을 나타내는 엔티티속성과 기능 수행을 위한 모듈들을 지닌다. 유저엔티티가 의뢰한 정보메세지는 서버엔티티들 사이의 송·수신 모듈기능을 통해 통신메세지의 한 원소로써 전송되며, 발신 유저엔티티가 수신 유저 엔티티에게 전달하고자 하는 정보와 이에 대한 제어 및 서비스 요청 정보를 포함하고 있다. 통신메세지는 송신 엔티티와 수신 엔티티 사이의 정보메세지 및 상호 정보교환을 위한 질의·응답 내용으로 구성된다.

■ 정의 1 메세지 처리시스템 *MHS*(Message Handling System)는 메세지를 이용하여 정보를 송·수신하는 유저엔티티 집합 *UE*(User Entity)와 메세지를 전달하고 서비스하는 전달시스템 서버엔티티 집합 *SE*(Server Entity)로 구성된다.

$$MHS = UE \cup SE,\ UE \cap SE = \phi$$

■ 정의 2 임의의 엔티티 $en \in UE \cup SE$은 엔티티 이름 *eid*, 엔티티 속성 집합 *EAT*, 모듈 집합 *EM*, 보안레이블 *esl*, 이웃엔티티와 연결함수 *CHF*, 정보메세지 집합 *EIM*으로 표현된다.

$en = (eid, EAT, EM, esl, CHF, EIM)$

*eid*는 엔티티가 *MHS*내에서 구별되는 유일한 이름이며, *EAT*는 *en*이 지니는 속성들로서 전체 속성 집합 $AT = \{at_1, at_2, \ldots, at_i, \ldots, at_n\}$의 부분집합이며, at_i = (attribute name, value)로 이루어진다. *EM*은 *en*이 가지고 있는 모듈들로써 통신 및 프로세싱기능을 수행한다. *esl*은 보안관리자가 엔티티 *en*에게 부여한 보안레이블로써 보안레이블 집합 *SL*의 멱집합중 한 원소이다. $esl \in 2^{SL}$로서 $esl = (sl_1, sl_2, \ldots, sl_i, sl_{i+1}, \ldots, sl_n)$가 되며, $sl_i < sl_{i+1}$일때 sl_{i+1}은 sl_{i+1}의직후자(immediate successor)이다. *CHF*는 채널로부터 이웃엔티티 및 연결된 현재 보안레이블로의 함수로써 채널집합을 *CH*라 할때 $ch \in CH$, $bsl \in 2^{SL}$에 대하여 $CHF(ch) = (eid, bsl)$이 된다. *EIM*은 *en*이 지니고 있는 정보메세지들의 집합이다.

■ 정의 3 통신메세지 *cm*은 송신 엔티티 *seid*, 수신 엔티티 *reid*, 메세지 타입 *mt*, 아그멘트 집합 *ARG*, 값 *v*로 구성된다.

$cm = (seid, reid, mt, ARG, v)$

seid, *reid*는 각각 송·수신 엔티티 이름을 나타내며, $mt \in \{bind, unbind, submit, transfer, delivery, report, admin\}$으로써 통신 액세스 타입을 표시한다. $ARG = \{arg_1, arg_2, \ldots, arg_i, \ldots, arg_n\}$, arg_i = (arg name, value)이며, 정보메세지와 연결 보안레이블 *bsl*은 하나의 아그멘트로서 전송된다. *mt*에 따라 정해진 *arg*들을 수신한 수신 엔티티는 *arg*에 대한 모듈을 수행하고, 얻어진 결과값 *v*를 응답한다. $bsl \in 2^{SL}$은 송신 엔티티가 수신 엔티티에게 연결하고저 하는 *seid*의 현재 보안레이블이다.

■ 정의 4 정보메세지 *im*은 발신 유저엔티티 *org*, 수신 유저엔티티 *rcp*, 메세지 이름 *mid*, 메세지 보안레이블 *msl*, 액세스 제어 정보 *aci*, 서비스 요청 *sr*, 정보내용 *cont*로 구성된다.

$im = (org, rcp, mid, msl, aci, sr, cont)$

org, *rcp*는 각각 *im*을 생성한 발신 유저엔티티 및 *im*을 수신할 수신 유저엔티티를 나타낸다. 실제로 하나의 *im*은 여러 *im*들의 집합으로 나타날 수 있으나, 단일 *im*의 반복으로 해석될 수 있으므로 여기서는 단일 *im*으로 간주한다. *mid*는 *MHS*내에서 정보메세지 *im*을 구별할 수 있는 유일한 이름이며, 메세지가 나뉘지는 경우, *im*의 *rcp*를 *rcp*(*im*)이라고 표현할 때 $rcp(im) = (rcp_1, rcp_2, \ldots, rcp_i, rcp_n)$인 모든 $i(1 < i < n)$에 대하여, rcp_i에게 전송되는 $mid(im) = mid + rcp_i$가 된다. *msl*은 *im*의 보안레이블로써 *SL*의 한 원소인 단일 보안레벨을 지닌다. 액세스 제어 정보 *aci*(access control information)는 메세지 발신 유저엔티티가 지정한 *im*의 액세스제어 정보로써 자격있는 엔티티만이 *im*을 액세스 할 수 있다. 복호화나 토큰등을 풀 수 있는 엔티티만이 *im*을 액세스할 수 있도록 제어하는 것이 한 예로 들 수 있다. *sr*은 메세지 발신 엔티티들이 서버엔티티에게 요청하는 서비스 요구이다.

■ 정의 5 엔티티 *en*의 정합 IF는 다음과 같은 함수들로 구성된다.

$IF = CMB \times MCB \times IMB \times MIB$

CMB : $ARG(cm) \rightarrow EM$는 통신메세지들을 해당되는 모듈과 연결시킨다.

MCB : $EM \rightarrow ARG(cm)$는 모듈의 결과를 응답메세지와 연결시킨다.

IMB : $SR(im) \rightarrow EM$는 수신된 정보메세지 *im*의 서비스 요청들을 해당모듈과 연결시킨다.

MIB : $EM \rightarrow EIM$는 모듈의 결과를 정보메세지와 연결시킨다.

정합 *IF*는 통신메세지나 정보메세지의 요구사

항을 검사하여 엔티티내의 모듈에 연결, 반대로 모듈들로부터의 결과 값과 메세지들을 연결하는 함수로 표현된다.

■ 정의 6 엔티티 모듈 $m \in EM$은 통신메세지 유한집합 CM과 정보메세지 유한집합 IM에 대한 처리 함수로 구성된다.

$$m = CMF \times IMF$$

$$CMF : ARG \rightarrow 2^{FAI \times V} \times 2^{SL} \times 2^{IM} \times 2^{CM}$$

$$IMF : SR \rightarrow 2^{IM} \times 2^{IIM \times ACI \times V} \times 2^{EIM \times CONT \times V}$$

CMF는 통신메세지의 아그멘트에 따라 수신 엔티티가 지닌 속성값을 변경하거나 송신이 설정한 연결 보안레이블 bsl에 따른 자신의 연결 보안레이블을 결정한다. 아그멘트가 정보메세지를 포함할 때, 수신 엔티티가 보유하는 정보메세지가 증가하게 된다. 수신된 통신메세지의 아그멘트를 수행한 후의 결과값에 따라 필요한 응답 통신메세지가 생성된다. IMF는 정보메세지가 요청하는 서비스요구 SR을 수행하며, 그 결과로써 메세지의 분배 및 통합을 발생하거나, 엔티티내의 정보메세지의 aci 및 $cont$내용을 변경하기도 한다.

3. 안전한 메세지 전달시스템 모델

3.1 보안레이블과 정보흐름

3.1.1 보안레이블

보안레이블은 레이블을 지닌 주체 또는 객체의 보안특성을 나타낸다. 주체의 보안레이블은 주체가 액세스할 수 있는 보안 처리능력을 나타내며, 객체의 보안레이블은 자신을 액세스하기 위하여 지녀야하는 필요조건을 나타낸다. 보안정책은 주체 및 객체의 보안레이블을 정의하고 어떠한 경우에 분류된 레이블에 의해 액세스가 허용되는가를 정의한다. 전형적인 군용 보안정책[5, 6]에서 보안레이블(security label)은 수직적인 보안등급(security level)과 수평적인 보안범주(security category)로 구분되며, 주체의 보안등급은 보안자격(security clearance)으로 객체의 보안등급은 보안분류(security classification)로 정의한다. 논문에서의 보안레이블은 보안등급과 보안 범주를 합친 강제적 레이블(Mandatory Label : ML)과 후술하는 임의적레이블(Discretionary Label : DL) 및 마킹레이블(MarKing Label : MK)을 포함한다. 여기서는 레이블이 지니는 특성 설명을 위해 보안레이블은 강제적 레이블로만 구성된다고 가정하여 레이블의 래티스(lattice)성질을 설명한다. 보안등급 집합 SL은 집합내의 임의의 두원소 sl_1, sl_2사이에 정렬순서(well ordering)관계를 지니는 전순서 집합이다. 관계 $\leq$는 임의의 두원소 사이의 지배(dominate)관계를 나타내며, $sl_1 \leq sl_2$라면 sl_1에서 sl_2로 정보가 흐를 수 있다. 보안 범주 집합 SC에 대해 SC의 모든 부분집합의 합집합 2^{SC}는 집합 포함관계에 의한 반순서 관계(partial ordering relation)를 지닌다. 즉, SC의 부분집합 SC_1이 다른 부분집합 SC_2에 포함된다면, $SC_1 \subseteq SC_2$, SC_2은 SC_1을 지배한다(dominate)고 한다. 보안레이블 집합 L은 보안등급 집합 SL과 보안범주 집합 SC의 멱 집합(power set)의 카테시안 곱(cartesian product)으로 표시되며 반순서 관계를 지닌다. $L = SL \times 2^{SC}$이며, L의 임의의 두원소 $l_1 = (sl_1, sc_1)$과 $l_2 = (sl_2, sc_2)$ 사이에 반순서 관계를 가진다.

예제 1 $SL = \{1,2\}$, $SC = \{group1, group2\}$라고 하고, 임의의 주체 보안레이블 $s_{sl} = (1, \{group1, group2\})$, 임의의 객체 보안레이블을 $o_{sl} = (2, \{group1\})$라고 했을 때, s_{sl}은 o_{sl}을 지배하며, $s_{sl} \geq o_{sl}$라고 표기한다.

3.1.2 액세스제어 목록(임의적 레이블)

객체의 소유자는 자신의 임의적인 의사에 따라 객체를 액세스할 수 있는 주체를 액세스제어 목록

(Access Control List : ACL)에 기록할 수 있다. 액세스는 기록된 주체의 *id*에 근거하여 읽기(read)시에는 비밀성 제어되며, 쓰기(write)시에는 무결성 제어된다. 전형적인 액세스제어 목록은 M_{ij} 메트릭스 형태를 가지며, M_{ij}의 한 원소(i, j)는 주체 S_i가 객체 O_j에 대하여 허용된 액세스형태를 나타낸다. 액세스 종류는 Multics[16]에서는 {*read*, *write*, *append*, *execute*}로, secure TUNIS에서는 {*read*, *write*, *execute*}로 통신모델에서는 {*connect*} 또는 {*send*, *receive*}로 시스템에 따라 다르게 해석하기도 한다. 액세스제어 목록에 지정된 주체는 객체에 대하여 지정된 액세스가 가능하다. 논문에서의 액세스 종류는 {*connect*, *send*, *receive*, *read*, *write*, *create*, *service request*}들로 구성되며, 연결목록 *conl*(connection list)와 수신 유저엔티티들을 임의적으로 연결 및 수신을 허용한 주체들의 집합을 나타내는 임의적레이블로 사용한다.

3.1.3 마킹레이블

보안레이블이나 액세스 제어 목록에 의한 제어 외에 때때로 문서의 배포 및 처리를 제한하거나 주의를 요하는 마킹을 중요문서에 부여하여야 할 필요가 있다. NOFORN(외국인에 제공금지), ORCON(생성자가 지정한 그룹에게만 문서의 배포 및 권한이양)[18], REL xx(xx기관 또는 국가에게만 제공)등이 그 예로써, 보안레벨에 의한 정보흐름 제어 또는 소유자가 지정한 주체 식별자(subject identification)에 의한 정보흐름 제어로써는 제공할 수 없는 보안 속성을 지닌다[15, 17, 18, 21]. 마킹레이블은 상기제어를 위한 마킹들의 집합으로 이루어지며, 상호 독립적 또는 중첩되어 사용된다. NOFORN과 REL의 예로써 "NOFORN/REL CAN"의 경우 외국인이지만 CAN국적은 허용됨을 의미하며 상호 독립적이면서 합쳐진 마킹제어를 요구한다. 이와같은 종류의 마킹레이블은 주체의 국적, 기관, 역할을 비교 근거로 하므로 액세스하는 주체의 속성을 필요로하며, 동일국적 또는 ORCON등과 같이 동일 그룹 개념의 레이블에 근거한 정보흐름을 요구한다[18].

3.2 메세지 전달시스템에서의 안전한 정보흐름

메세지 전달시스템은 발신 유저엔티티가 의뢰한 정보메세지를 발신 유저엔티티가 지정한 수신 유저엔티티에게 전달하는 서버시스템이다. 전달시스템 보안정책은 서버엔티티들 사이에 메세지를 안전하게 전달하는 것이 그 목적이며, 따라서 엔티티와 엔티티 사이의 메세지 전송시, 송·수신 엔티티가 필요한 보안요구조건을 만족하는가 또는 서비스 프로세싱 수행시 메세지를 통하여 경로상의 엔티티가 요구한 서비스 요구조건을 만족하는가를 참조 모니터해야 한다. 전달시스템은 MLS(Multi Level Security)의 강제적 보안정책, 임의적 보안정책, 마킹 보안정책을 통신환경에서 준수함으로써 허가되지 않은 정보메세지의 전달흐름을 방지한다. 유저환경에서 보는 전달시스템은 하나의 서버엔티티로 간주할 수도 있으며, 서버엔티티들의 집합으로 보고 각 서버엔티티에게 유저의 보안레이블을 부여함으로써 유저엔티티로 간주할 수도 있다. 유저의 보안정책은 유저메세지의 안전한 전달과 비인가자로의 정보흐름 방지가 그 목적이며, 따라서 유저엔티티와 유저엔티티 사이의 메세지 전달 및 유저엔티티의 메세지 액세스시, 필요한 보안조건을 만족하여야 한다. 그러나, 유저엔티티가 멀리 떨어져 있는 다른 유저엔티티에게 메세지를 통한 정보전달을 원할 때, 유저엔티티는 메세지 전달시스템에게 전달서비스를 요청하게 된다. 만일 유저엔티티가 전달시스템 자체를 완전히 믿을 수 없다고 가정할 때, 유저엔티티와 전달시스템 경로상의 모든 서버엔티티 사이에 1:1질의·응답 확인 절차를 거치거나, 서버엔티티를 유저환경내에 포함함으로써 유저의 보안정책을 준수토록 하여야 한다. 물론, 서버엔티티 모두를 유저엔티티들로 포함된다면, 유저전용 전달시스템이 구성될 수도 있으나, 전달시스템의 본래 서비스 목적과

부합되지 않는다. 본 논문에서는 서버엔티티에게 유저환경의 보안레이블을 부여함으로써, 전형적인 컴퓨터 시스템 보안에서와 같이 유저엔티티의 메세지 액세스 관계로써 해석한다. 전달시스템의 또 다른 특성은 서버엔티티가 전송기능과 서비스 프로세싱기능을 병행해야 하므로 메세지의 흐름이 수신-처리-송신의 정보흐름 특성을 지닌다는 것이다. 발신 유저엔티티가 전송 의뢰한 정보메세지는 발신 유저엔티티가 부여한 유저환경에서의 보안속성을 지님과 동시에 발신 서버엔티티가 전송 서비스를 위해 부여한 서버환경의 보안속성을 지니게 된다. 따라서, 정보메세지가 임의의 한 엔티티로부터 다른 엔티티로 전송 및 처리된 후 또다른 엔티티로 재 전송될 때, 다음의 보안요구조건을 만족하여야 한다.

1. 송신 엔티티와 수신 엔티티사이의 전송 보안조건
2. 정보메세지가 요구하는 송신 보안조건
3. 정보메세지가 요구하는 수신 보안조건
4. 서버엔티티가 정보메세지를 프로세싱하기 위하여 필요한 보안조건

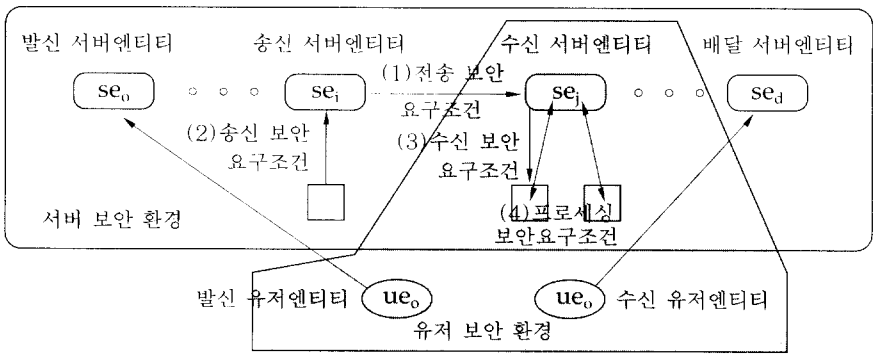


그림 1. 서버 및 유저 환경과 보안요구조건

서버 및 유저환경에서 필요한 보안정책은 전형적인 액세스제어 정책인 강제적제어(Mandatory Access Control : MAC) 및 임의적 제어 (Discretionary Access Control : DAC)와 [5,6] 와 최근에 제기되고 있는 마킹제어(Marking Access Control)[2,3] 정책을 따른다. 보안정책은 전술한 보안레이블(강제적 레이블 ML : Mandatory label), 임의적레이블(DL : Discretionary Label), 마킹레이블(MK : MarKing)에 근거하여, 주체 및 객체 사이의 액세스를 참조 모니터함으로써 구현된다. 보안정책에 의해 정의되는 보안레이블 $L = ML \times DL \times 2^{MK}$형태의 카테시안 곱으로 구성된다. ML은 보안등급 집합 SL의 멱집합과 보안범주 집합 SC의 멱집합의 카테시안곱으로 구성되는 반순서집합이다. SL = {1급, 2급, 3급}이라고 할때, ML의 첫번째 원소는 2^{SL} = {{1급}, {2급}, {3급}, {1급, 2급}, ..., {1급, 2급, 3급}}중의 하나이다. DL = {엔티티 이름, 액세스 타잎}로써 지정된 액세스를 허용함을 나타낸다. MK = {mk_1, mk_2, ..., mk_i, ..., mk_n}로써 보안정책에서 정의한 마킹레이블들의 집합으로 표현된다. 서버엔티티에 부여되는 보안레이블 l은 서버 보안레이블 $sl \in L$과 유지 보안레이블 $ul \in L$의 순서쌍(ordered pair)로써 구성되며, 서버엔티티 se_i의 보안레이블을 $l(se_i)$로 표현할 때, $l(se_i) = (sl(se_i), ul(se_i)) = (\{sml(se_i), sdl(se_i), smk(se_i)\}, \{uml(se_i), udl(se_i), umk(se_i)\})$이 된다. 여기서 sxx와 uxx는 각각 서버 및 유저의 보안레이블을 구성하는 강제적, 임의적, 마킹레이

블임을 표시하며, sxx와 uxx를 합쳐 xx라고 표시한다. 정보메세지 im에 부여되는 보안레이블은 ml (sml 및 uml)이 단일 보안등급과 단일 보안범주인 것을 제외하고는 서버엔티티의 보안레이블과 동일하다. 4장에서 제안된 메세지 훨타 알고리즘에서 사용되는 보안레이블은 정적 보안레이블과 동적 보안레이블로 확장된다. 정적 보안레이블은 엔티티에 초기에 부여된 ml, dl, mk외에 특권 pr(PRivilege)을 포함하며, 동적 보안레이블은 정보 메세지로부터 승계받은 현재 보안레이블 cml, cdl, cmk외에 함수 수행결과로써 얻어진 액새스권한 right를 포함한다. 특권이 엔티티나 메세지에 관련된 보안레이블인 것에 반해, 액세스권한은 정보메세지가 요구하는 서비스를 수행하기 위해 사전에 엔티티가 가져야 할 조건으로 서비스에만 관련된다.

3.2.1 엔티티와 엔티티사이의 정보흐름

서버엔티티 se_i가 통신메세지 $cm = (se_i, se_j, mt, arg, v)$를 다른 서버엔티티 se_j에게 전송하는 것을 $se_i \rightarrow se_j$으로, 엔티티 se의 강제적 레이블 ml을 $ml(se)$로, 임의적레이블 dl을 $dl(se)$과 같이 표현할때, 엔티티와 엔티티사이의 정보흐름은 다음과 같은 조건을 만족할 때 안전하다.

(연결 강제적 조건) $sml(se_i) \cap sml(se_j) \neq \phi$이고 엔티티의 현재 강제적 레이블을 cml이라 할 때, $cml(se_i) \leq ml(se_j)$이고 $cml(se_j) \leq ml(se_j)$일때 se_i와 se_j는 연결 가능하다. 서버엔티티의 연결은 송·수신 엔티티사이의 연결가능한 강제적레이블이 존재할 때 가능하며 각 엔티티의 현재 강제적레이블은 엔티티가 지닌 보안처리능력 ml에 의해 지배되어야 한다. 만일 $ml(se_i) \cap ml(se_j) = \phi$이거나, $cml(se_j) \geq ml(se_j)$인 경우 주어진 보안 처리능력이상의 메세지가 전송될 수 있음을 의미한다. 이 조건은 서버 환경에서만 구현되므로 ml과 cml은 각각 sml과 $csml$로 대응된다.

(연결 임의적조건) $se_i \in conl(se_j)$이고 $se_j \in conl(se_i)$

$se_i \rightarrow se_j$시 se_i와 se_j는 각각 상대방 연결제어 목록의 한 원소이어야 한다.

3.2.2 서버엔티티와 메세지 사이의 정보흐름

송신 서버엔티티 se_i가 정보메세지 im_i를 cm_n의 한 부분으로 송신코저 할 때 송신 서버엔티티 se_i는 서버 및 유저 보안정책을 준수함과 동시에 정보메세지 im_i에서 요구하는 송신조건을 만족하여야 한다. 서버시스템의 강제적, 임의적조건은 2.1절의 송·수신 엔티티 사이에서 정의되었으나, 마킹 요구조건은 객체가 주체의 자격여부를 검사한다는 관점에서 정보메세지 im과 송·수신 서버 엔티티 사이의 관계로 해석한다. 먼저 정보메세지 $im_i = im(se_i)$가 전송메세지가 되기 위해 정보메세지 im_i가 요구하는 보안조건을 정리하면 다음과 같다.

1. 송신 서버엔티티는 정보메세지를 송신할 수 있는 강제적레이블을 지녀야 한다.
2. 송신 서버엔티티는 경로상의 엔티티가 지정한 엔티티에게 정보메세지를 송신할 수 있다.
3. 송신 서버엔티티는 정보메세지가 지닌 마킹조건을 갖춘 엔티티에게 정보메세지를 송신할 수 있다.
4. 송신 서버엔티티는 경로상의 엔티티가 요구하는 자격있는 엔티티에게 정보메세지를 송신할 수 있다.

이상의 송신 보안요구조건이 만족될 때 송신 서버엔티티가 정보메세지 im_i를 수신 서버엔티티에게 전송할 수 있다. 컴퓨터 시스템에서와 같이 단일 운용환경에서는 송·수신 엔티티를 동시에 참조 모니터할 수 있으나, 메세지 전달시스템과 같은 분산 환경에서는 송신측과 수신측의 질의 응답과정을 거치거나 믿을 수 있는 시스템 서버의 서비스를 통하여 상기조건을 감시하여야 한다. 시스템 입장에서 전송은 하나의 원시 액세스이며, 송신 보안요구조건이 수신시 검사되더라도 보안정책은

동일하게 준수된다고 할 수 있다. 모델에서는 실제 환경을 감안하여, (1,2)는 송신시의 (1,3,4)는 수신시의 보안요구조건으로 분리한다. 전술한 바와같이 유저입장에서 본 서버엔티티는 발신 유저엔티티와 서버엔티티의 1:1관계로써, 정보메세지를 수신할 때 상기조건을 만족해야 한다.

송신 서버엔티티와 메세지 사이의 정보흐름

(송신 강제적조건 1) $cml(se_i) \leq cml(se_j)$

$se_i \rightarrow se_j$시 se_i와 se_j사이에 전송 가능한 현재 강제적레이블 cml이 존재하여야 하며, se_j가 수신할 수 없는 im_i의 송신을 제한한다. 만일 $cml(se_i) \geq cml(se_j)$의 경우, $ml(im_i) \geq cml(se_j)$인 im_i가 전송될 수 있다.

(송신 강제적조건 2) $sml(im_i) \leq cml(se_i)$

단일 보안레이블을 지니고 있는 정보메세지 im_i는 se_i현재 강제적 레이블의 한 원소이어야 한다. 이때 (송신 강제적조건1)에 의해 $sml(im_i) \in cml(se_i) \leq cml(se_j)$이므로 $sml(im_i) \in cml(se_j)$가 된다. $uml(im_i)$는 발신 유저엔티티와 수신 서버엔티티 사이의 관계로써 수신시 조사된다.

(임의적 송신조건) $se_j \in dl(im_i)$

se_j는 수신 서버엔티티 또는 수신 유저엔티티로써, 발신 엔티티가 지정한다. 발신 유저엔티티가 수신 서버엔티티를 지정한다함은 발신유저 엔티티가 신뢰할 수 있는 서버 엔티티의 경유를 의미한다. 따라서, n개의 수신 엔티티가 존재할 때, 송신엔티티는 $se_j \in dl(im_i)$인 엔티티에게만 정보메세지를 송신하여야 한다.

수신 서버엔티티와 메세지 사이의 정보흐름

(수신 강제적조건) $uml(im_{ij}) \leq uml(se_j)$

수신 서버엔티티 se_j가 유저 환경의 강제적레이블 uml을 지닌다면, se_j의 보안처리능력은 $uml(im_{ij})$를 지배하여야 한다.

(수신 마킹조건) $mk(im_{ij}) \leq mk(se_j)$

수신 서버엔티티 se_j는 서버 및 유저 환경에서 요구하는 마킹레이블에 부합되는 엔티티일때 정보메세지 im_{ij}를 수신할 수 있다.

(수신 자격조건) $pr(im_{ij}) \leq pr(se_j)$

수신 서버엔티티 se_j는 서버 및 유저환경에서 요구하는 특권레이블을 지녀야 한다.

3.2.3 메세지와 메세지 사이의 정보흐름

정보메세지 im_i가 임의의 엔티티 se_j에게 수신되었다는 것은 se_j가 im_j를 처리할 수 있는 유저 및 서버 보안정책이 요구하는 강제적, 임의적, 마킹, 특권 자격을 갖추었음을 뜻한다. 그러나, 이는 im_j가 지닌 정보 그 자체에 대한 자격조건이며, 이 정보를 어떻게 프로세싱하는가에 대한 제어조건은 아니다. 프로세싱은 통신처럼 메세지 전체에 대한 액세스가 아닌 서비스 요구별 기능수행을 의미하며, 서비스 요구에 따라 필요한 특권이나 권한조건을 요구한다. 이러한 조건은 단순히 하나의 서비스요구에 따른 특권 요구뿐 아니라 서비스를 수행하기 이전에 다른 기능의 수행 완료를 요구하기도 한다. Sandhu는 후자의 경우를 변형된 액세스 권한이라 정의하여, 여러 주체가 지닌 역할에 따라 기능 수행을 완료할 때 액세스 권한이 변형된다는 모델[13]을 제안하였다. 본 논문은 액세스권한의 변형 자체가 곧 정보의 모든 권리를 가지지 않는다는 점에서 다르다. 간단히 말해서 제안된 모델은 정보를 액세스할 수 있는 권한을 얻더라도 정보의 흐름은 후술하는 승계 속성을 지닐 것을 요구한다. 따라서, 정보메세지에 대한 엔티티의 액세스는 액세스 권한 조사를 통과하여야 하며, 동시에 정보메세지가 지닌 레이블 속성을 승계할 것을 요구한다. 메세지에서 메세지로의 정보흐름은 주체엔티티를 경유하여 발생되므로 소스메세지의 레이블은 read시 주체엔티티에게 승계되어 write시 종착메세지가 요구하는 자격조건과 비교된다. 이때의 자격조건은 지금까지 설명한 다중 보안레이블 개념이 아닌 단일 보안레이블 개념에 의해 객체, 주체, 객체의 관계에서 참조 모니터 된다.

(정보흐름 강제적조건) $ml(im_j) \leq ml(im_k)$

(정보흐름 임의적조건) $dl(im_j) \leq dl(im_k)$

(정보흐름 마킹조건) $mk(im_j) \leq mk(im_k)$

(정보흐름 자격조건) $pr(im_j) \leq pr(im_k)$ im_j보다 im_k의 강제적, 임의적, 마킹, 특권레이블이 높을 때 정보는 흐를 수 있다. 만일 se_i가 im_j의 정보를 낮은 보안레이블을 지닌 im_k에게 불법적으로 전달하더라도 im_k가 im_j의 보안레이블을 승계한다면, im_k를 처리할 수 있는 주체는 im_j이상의 자격을 지녀야 한다.

(프로세싱 자격조건) $pr(se_j) \geq pr(sr(im_j))$이고 $right(se_j) \geq right(sr(im_j))$

se_j가 im_j의 서비스 요구가 필요로하는 특권이나 권한을 지녔을때 im_j를 프로세싱할 수 있다. 프로세싱은 메세지와 메세지간의 정보흐름이 아닌 메세지와 엔티티 사이의 액세스이지만 엔티티가 정보를 흘릴 수 있는 잠정적인 정보흐름이다.

4. 메세지 훨터 알고리즘

정보메세지가 발신 유저엔티티로부터 수신 유저엔티티에게 안전하게 전달되기 위해서는 전달시스템이 안전해야 한다. 전달시스템이 안전하다는 것은 전술한 메세지 전달시스템 모델에서 추구하는 보안정책과 유저가 추구하는 보안정책이 동시에 만족해야 한다. 임의의 서버엔티티는 서버 환경의 한 구성요소로써 이웃 서버엔티티와의 1:1 관계와 경로상의 서버엔티티들과의 1:n계를 지니며, 동시에 유저엔티티와 1:1서버 관계를 유지한다. 메세지와 메세지 사이의 관계에 대하여 유저, 엔티티, 유저의 1:1:1의 관계를 지닌다. 따라서, 서버엔티티는 서버 및 유저 환경에서 주어진 보안속성인 강제적, 임의적, 마킹 특권레이블이 보안정책에 부합될 때 정보메세지에 대한 액세스가 허용된다. 제안된 메세지 훨터 알고리즘은 서버 엔티티가 정보메세지를 액세스할 때, 서버엔티티의 액세스를 제어하는 보안 메카니즘에 대한 알고리즘이다. 서버엔티티의 정보메세지에 대한 액세스는 연결, 전송, 프로세싱의 3단계로 나누어지며 액세스가 허용될 때마다 서버엔티티의 보안상태 천이가 발생된다. 알고리즘은 그림 2와 같이 크게 정보메세지 전체에 대한 액세스 특권 조사와 정보에 대한 액세스 권한 조사로 이루어지며, 메세지 전송시 송·수신 엔티티와 정보메세지 사이의 관계와 수신된 정보메세지와 액세스하는 서버엔티티 사이의 관계로 나타난다.

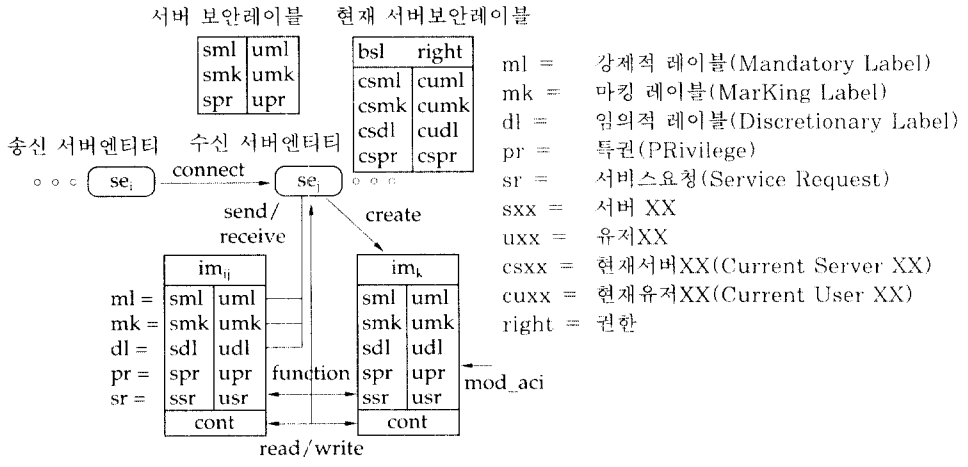


그림 2. 메세지 훨터의 대상 액세스 및 보안 레이블

4.1 연결단계

서버시스템의 임의의 두 엔티티 se_i가 se_j에게 정보메세지를 전달하고저 할 때, se_i와 se_j는 서버시스템이 요구하는 보안정책을 준수하여야 한다. 만일 se_j가 강제적레이블 sml을 지녔다면 (CO1), se_i는 자신의 sml범주내에서 상태 엔티티와 연결되어야 한다(CO2). 연결은 어떤 엔티티던지 시도할 수 있으며, 현재 연결레이블 bsl은 독립적으로 제안될 수 있다. 연결시도를 수신한 엔티티 se_j는 강제적 레이블을 지녀야 하며 제안된 bsl은 자신의 sml범주내에 속하여야 한다(CI1, CI2). se_i와 se_j사이의 bsl 설정은 상호 승인에 의해 이루어지며, $sml(se_i) \geq bsl(se_j)$의 관계를 지님으로써 se_j가 처리할 수 있는 레이블 범주내에서 se_i와 연결될 수 있다. 이웃 엔티티와의 연결은 연결목록 내의 개별 엔티티 이름으로 허용(때로는 금지)될 수 있으며, 연결시도 엔티티 입장에서는 보안성을 얻기 위하여, 연결이 요청되는 엔티티 입장에서는 무결성을 얻기 위한 수단으로 사용될 수 있다(CO3, CI3). 송·수신 엔티티가 상호 믿을 수 없는 환경이라면, 각 엔티티는 상대를 인증하기 위한 인증 절차를 거치게 된다(CO5, CI4). 상대에 대한 인증표는 각 엔티티가 보관하고 있거나 인증 센터로부터 수신받아 인증절차를 수행할 수 있다. 엔티티의 상태 변경 (CO4, CI5, CO9)은 보안속성의 비교 또는 액세스 성공시 이루어지며, state(se)는 엔티티의 현재 보안상태를 나타낸다.

CASE 1 : connect_out (se_i, $cert$, bsl)
(CO1) if ($sml(se_i)$)
/* se_i는 보안레이블을 지닌 엔티티 */
(CO2) if ($sml(se_i) \geq bsl(se_i)$) :
/* se_i의 최대와 현재 보안레이블 비교 */
(CO3) if ($se_i \in conl(se_i)$)
/* se_i는 연결허용 엔티티 */
(CO4) state(se_i) =(connect out, se_i, bsl)
/* cm_{ij}는 se_i에게 전송 */

CASE 11 : connect_out_result(se_i,cm_{ji})
(CO5) if($cert(se_j) = cert(cm_{ji})$)
/* se_j를 신분인증 */
(CO6) state(se_i)
= (connect_out_resut, se_j,bsl)
/*se_i는 se_j와 bsl연결상태 */
(CO7) if ($sml(se_i) \geq bsl(cm_{ji})$)
(CO8) state(se_i) = (connect, se_j, $bsl(cm_{ji})$)

DASE 2 : connect in (cm_{ji})
(CI1) if ($bsl(cm_{ji})$)
/*se_i, se_i는 보안레이블을 지닌 엔티티*/
(CI2) if ($bsl(cm_{ji}) \leq sml(se_i)$)
/*se_j가 se_i에게 $bsl(cm_{ji})$로 연결시도 */
(CI3) if ($se_i \in conl(se_i)$)
/*se_i는 연결 허용 엔티티 */
(CI4) if ($cert(se_j) = cert(cm_{ji})$)
/*se_j를 신분인증*/
(CI5) state (se_i) = (connect, se_i, $bsl(cm_{ji})$)
/* se_j는 se_i와 bsl연결상태 */

4.2 전송단계

se_i와 se_j사이의 정보흐름은 낮은 레벨에서 높은 레벨로 발생될 때 안전하다. 연결단계가 무방향성인 것에 비해 메세지전송은 방향성을 지니므로, se_i와 se_j가 강제적레이블을 지니고 se_i가 se_j에게 im_{ij}를 송신할 때 (SD2)를 만족하여야 한다. 만일 se_i와 se_j가 bsl을 독립적으로 설정할 수 있고, $sml(se_i) \geq sml(se_j)$이고 $bsl(se_i) \geq bsl(se_j)$일때, $bsl(se_i) \geq sml(im_{ij}) \geq bsl(se_j)$인 정보메세지 im_{ij}가 se_j로 송신될 수 있다. 따라서, 서버엔티티들이 지닌 강제적 레이블 $sml(se_i)$ 및 $sml(se_j)$과 현재 강제적레이블 $bsl(se_i)$ 및 $bsl(se_j)$ 사이에 (CO2, CI2, SD2)가 우선 만족하고, 송신 서버엔티티의 현재 강제적레이블 $bsl(se_i)$와 정보메세지 레이블 $sml(im_{ij})$사이에 (SD3)조건이 만족된다면, 송신 서버엔티티 se_i는 수신 서버엔티티 se_j에게 정보메세지 im_{ij}를 전송할

수 있다. 서버시스템에서의 강제적 정보흐름은 송·수신 엔티티 se_i, se_j와 im_{ij}사이에서 제어되지만, 만일 se_i나 se_j가 유저 강제적레이블 uml을 지닌다면, 발신 유저엔티티가 부여한 $uml(im_{ij})$과 유저환경에서의 강제적 액세스제어가 이루어져야 한다. uml을 지닌 서버엔티티사이의 메세지 전송 제어 역시 서버시스템의 강제적 정보흐름 제어와 동일하게 적용될 수 있으나, 유저엔티티는 서버엔티티의 전송 서비스에 의존한다는 관점에서 유저 엔티티대 유저 역할을 부여받은 서버 엔티티 관계로 정의한다. 따라서, uml을 지닌 서버엔티티는 발신 유저 엔티티와 1:1관점에서 액세스제어 된다 (RV3). 전달시스템 보안정책이 마킹제어를 포함하고 정보메세지 im_{ij}의 마킹레이블이 존재한다면, se_j는 정보메세지를 수신할 수 있는 마킹레이블을 소지하여야 한다. $mk(im_{ij}) = smk(im_{ij}) \oplus umk(im_{ij})$로써, $smk(im_{ij})$와 $umk(im_{ij})$는 각각 서버시스템 및 유저의 마킹레이블을 나타낸다. $\oplus$는 두 레이블이 비교가능할 때 높은 레이블을 취하며, 비교할 수 없을 때는 독립적으로 사용됨을 나타낸다. se_j는 서버시스템과 유저시스템에서의 마킹역할을 동시에 부여받으며, (RV5)와 (RV7)을 만족할 때, im_{ij}를 수신할 수 있다. 서버시스템의 마킹제어는 송신서버 엔티티가 정보메세지를 배포하기 전에 수신 서버엔티티의 마킹레이블을 알아야 하나, 분산 특성상 수신엔티티가 수신할 때 마킹제어가 이루어진다. 서버시스템에서 송신엔티티가 발신 유저엔티티의 마킹요구를 대리 수행함에 반해, 발신 유저엔티티가 의뢰한 유저 마킹레이블은 강제적 제어시와 마찬가지로 1:1관점에서 (RV7)을 만족할 때, se_j가 수신할 수 있다. 송신되는 정보메세지 im_{ij}는 발신 유저엔티티와 발신 서버엔티티가 지정한 수신 유저엔티티 및 전달 경로 서버엔티티를 포함한다. 전달 경로 서버엔티티의 지정은 강제적 제어나 마킹 제어와 달리 개별 엔티티를 명시 또는 함축적으로 지정한다. 따라서, 정보메세지를 송신하려는 송신엔티티 se_i는 se_j가 $sdl(im_{ij})$의 한 원소일 때 송신이 허용된다. $udl(im_{ij})$는 발신 유저엔티티가 직접 서버엔티티를 지정하는 경우나 지정된 수신 유저엔티티를 의미한다. 발신 유저엔티티로부터 전달되는 정보메세지는 경로상의 엔티티들이 수신엔티티에게 요구하는 조건을 담을 수 있다. 수신엔티티는 정보메세지를 수신하기 위해, 이러한 요구조건들(RV11, RV13)을 메세지 단위로 만족하여야 한다. 수신엔티티가 경로상의 엔티티를 믿지 못하여 메세지의 무결성을 조사하는 것도 동일한 개념으로 해석한다. 전송단계의 송·수신 엔티티의 상태 변경은 각 레이블에 대한 비교 및 액세스 성공시에 발생되며 특히 메세지의 송·수신은 엔티티가 보유하고 있는 정보메세지의 증감으로 나타낸다.

CASE 3 : send(se_i, im_{ij})

(SD1) if ($bsl(se_i)$)

/* 보안레이블을 지닌 연결 */

(SD2) if ($bsl(se_i) \leq bsl(se_j)$)

/*se_i와 se_j사이의 SMAC*/

(SD3) if ($bsl(se_i) \geq sml(im_{ij})$)

/*se_i와 im_{ij}와의 SMAC*/

(SD4) state (se_i)

= (send (SMAC), se_j, im_{ij})

(SD5) if ($se_j \in sdl(im_{ij})$)

/* 경로상 엔티티의 DAC*/

(SD6) state (se_i) = (send(SDAC), se_j, im_{ij})

CASE 4 : receive(se_i, im_{ij})

(RV1) if ($bsl(se_i)$)

(RV2) state (se_j)

= (receive (SMAC), se_i, im_{ij})

/* se_j와 se_i사이의 SMAC*/

(RV3) if ($uml(se_j)$ and ($uml(se_i) \geq uml(im_{ij})$)

/* se_j와 im_{ij}사이의 UMAC*/

(RV4) state (se_j)

= (receive(UMAC), se_i, im_{ij})

(RV5) if ($smk(se_j)$ and ($smk(se_i) \geq smk(im_{ij})$)

/*se_j와 im_{ij}사이의 SMKC*/

(RV6) state (se_j)

= (receive(SMKC), se_i, im_{ij})

(RV7) if ($umk(se_i)$ and ($umk(se_i) \geq umk(im_{ij})$)

/*se_i와 im_{ij}사이의 UMKC*/

(RV8) state (se_i)

= (receive (UMKC), se_i, im_{ij})

(RV9) if ($se_i \in udl(im_{ij})$)

(RV10) state(se_i)

= (receive(UDAC), se_i, im_{ij})

/*se_i와 im_{ij}사이의 UDAC */

(RV11) if (($spr(im_{ij})$)and ($spr(im_{ij}) \leq spr(se_i)$))

(RV12) state(se_i)

= (receive(SPAC), se_i, im_{ij}),

/*se_i의 privilege제어*/

(RV13) if($upr(im_{ij})$ and ($upr(im_{ij}) \leq upr(se_i)$))

(RV14) state(se_i)

= (receive(UPAC), se_i, im_{ij})

4.3 프로세싱 단계

연결단계에서 서버엔티티와 서버엔티티간에 정복 흐를 수 있는가 하는 사전조사가 엔티티에 부여된 강제적, 임의적, 신분확인 보안속성에 의해 이루어지며, 전송단계에서는 각 서버엔티티에서 설정한 *bsl*과 정보메세지 사이의 전송제어와 정보메세지가 요구하는 1:1또는 n:1조건들을 수신엔티티가 지녔는가에 대한 제어가 발생한다. 연결 및 전송단계의 액세스가 허용됨은 서버 및 유저의 보안정책이 정보 메세지를 통해 송·수신 엔티티사이 및 각 엔티티 단위로 준수되었음을 의미한다. 따라서, 전송되는 정보 메세지 im_{ij}는 수신 엔티티 se_i내의 정보메세지 im_i로 위치할 수 있고, 수신엔티티는 발신 유저 및 서버엔티티가 요청한 서비스를 수행할 수 있음을 의미한다. 서비스의 수행은 필연적으로 정보메세지내의 정보흐름을 유발시키며, 정보흐름을 일으킬수 있는 직접적인 액세스와 액세스하기 위하여 필요한 조건이 프로세싱 단계에서의 제어 대상이 된다. 직접적인 액세스로는 정보 그 자체에 대한 read/write 액세스, 액세스 제어 정보 *aci*에 대한 수정 액세스, 메세지의 생성에 대한 create 액세스가 있다. 액세스 필요조건으로는 서버엔티티 se_i가 서비스를 수행하기 위한 특별한 권리를 지녔는가 또는 선행되어야할 기능을 완료하였는가에 대한 function 액세스가 포함된다. 그림 3에서 주체 서버엔티티 se_i와 객체 정보메세지 im_i와 im_k사이의 프로세싱 제어를 보인다.

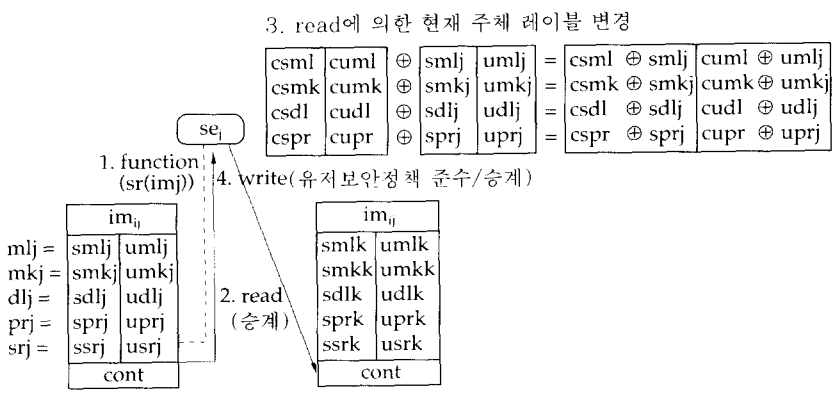


그림 3. 프로세싱 정보흐름

se_j가 im_i를 액세스하려면 se_j는 im_i에서 요구하는 조건을 만족하여야 한다. 만일 im_i의 aci를 변경하려면 (PM1)을 만족하여야 하며, 서비스를 위한 액세스시에는 (PF1, PF2)를 만족하여야 한다. 원시 액세스 read액세스를 시도하여 write액세스를 수행한함은 im_i부터 im_k로의 정보흐름이 발생함을 의미하며, 서버의 read액세스는 이미 연결 및 전송단계에서 허용되었기 때문에 프로세싱 단계에서 read에 대한 제어는 소스메세지의 보안레이블 승계속성만 유지시킨다. 그러나, write액세스는 실질적인 정보흐름의 발생이며, 이때의 정보흐름은 유저와 전달시스템의 보안정책에 따라야만 한다. 만일, 엔티티가 유지 보안레이블을 지녔다면, write액세스는 유저 보안정책 $ul(se_j) \leq ul(im_k)$조건을 만족하여야 하며, 그렇지 않을 때는 $ul(im_k) = ul(se_j) \oplus ul(im_k)$이 된다. 알고리즘의 $\leq$ / $\oplus$는 엔티티가 ul을 지닐 경우의 액세스제어 $\leq$와 그렇지 않은 상한(upper bound) 레이블을 승계하는 $\oplus$를 합친 의미이다. 서버 레이블의 경우 역시 $\leq$ / $\oplus$ 액세스제어에 포함된다. 만일, 유저와 서버의 보안레이블이 비교가능하다면 $\oplus$가 두 레이블 사이에 존재할 수도 있다.

CASE5 : read (im)
- (PR1) $cml(se) \leftarrow cml(se) \oplus ml(im)$
- (PR2) $cmk(se) \leftarrow cmk(se) \oplus mk(im)$
- (PR3) $cdl(se) \leftarrow cdl(se) \oplus dl(im)$
- (PR4) state (read, im)

CASE6 : write(im)
- (PW1) $cml(se) \leq / \oplus ml(im)$
- (PW2) $cmk(se) \leq / \oplus mk(im)$
- (PW3) $cdl(se) \leq / \oplus dl(im)$
- (PW4) $cpr(se) \leq / \oplus pr(im)$
- (PW5) state (write, im)

CASE7 : create(im)
- (PC1) $ml(im) \leftarrow cml(se)$
- (PC2) $mk(im) \leftarrow cmk(se)$
- (PC3) $dl(im) \leftarrow cdl(se)$
- (PC4) $pr(im) \leftarrow cpr(se)$
- (PC5) state(EIM + im)

CASE8 : mod_aci (im)
- (PM1) $pr(se) \geq aci(im)$
- (PM2) state (mod_aci, im)

CASE9 : function ($sr(im)$)
- (PF1) $pr(se) \geq pr(sr(im))$
- (PF2) $right(se) \geq right(sr(im))$
- (PF3) state(sr, im)

5. 관련 연구 비교

5.1 CCITT 및 ISO 보안연구와의 비교

X.400 보안 서비스[1]는 비밀성, 무결성, 신분인증, 부인봉쇄, 증명에 관한 프로토콜과 아그멘트를 규정하고 서비스 절차에 대하여 권고하고 있다. 또한, 보안레이블 = (보안 등급, 보안 범주, 프라이버시마크)로 정의하고, 구체적인 보안레이블 적용은 구현자에게 위임하고 있다. 프로토콜의 경우, 엔티티와 엔티티 사이의 1:1관계의 상호 신뢰할 수 없는 관점에서 X.509[2]의 암호화 기법을 이용하여 서비스를 제공하며, 서비스의 경우는 구체적인 절차에 관한 규정은 생략되었다.

본 논문에서는 전자의 경우를 특권 및 권한 액세스로 정의하여 포함하였고, 후자의 경우에는 전술한 강제적, 임의적, 마킹레이블로 구체화시켰다. 아울러, 유저 보안환경을 서버엔티티에 분산 적용함으로써 2가지 보안 정책이 준수될 수 있도록 제안하였다.

ISO액세스 제어 프레임 워크는 엔티티와 엔티티 사이에 액세스 제어 정보 및 액세스 제어 정보를 송·수신하되, 정보를 주체의 권한으로 보는가 또는 객체의 요구조건으로 보는가 아니면 두가지의 혼합으로 보는가에 따라 시스템 모델을 정의하고, 비교 검토하는 방법에 따라, 규칙 제어 방식 및 신분제어 방식으로 구분한다[3]. X.400의 경우와 마

찬가지로 보안 정책의 구현을 위한 구체적인 사항은 제시하지 않았다.

논문은 ISO의 보안레이블이 엔티티 및 정보메세지 모두에게 부여되는 강제적 규칙 제어방식과 신분에 근거하는 임의적 제어 방식을 모두 사용한다. 따라서, CCITT및 ISO보안 연구에서 제시하는 표준을 채택하여 구체화하며, 동시에 유저 보안정책을 독립적 또는 부가적으로 포함한다.

5.2 컴퓨터 액세스 제어 모델과의 비교

기존의 액세스 제어 모델은 대부분이 프로세스 주체의 화일 객체에 대한 액세스가 과연 권한이 있는가에 목적이 있었다. 따라서, BLP모델을 위시한 MLS환경의 모델들은 미시적 비밀성 보안정책인 강제적, 임의적 액세스 제어에 국한되었다. 유사한 관점으로 무결성 보안 정책을 위한 Biba[17], CW[18] 모델등도 이러한 범주에 속한다. 운용환경에서 제기된 마킹 보안을 모델화하는 제3의 모델이 제안되면서부터 다양한 모델들을 하나의 종합 모델로 해석하기 위한 연구가 [5,15]에 의해 시작되었다. 원시적인 읽기, 쓰기 등의 액세스의 관점에서 벗어나 서비스 수행을 위한 Sandhu의 타임 액세스 제어 모델[12] 및 액세스 변형 모델[13] 등이 상위 레벨의 액세스 제어를 위해 제안되었다. 제안된 알고리즘은 원시적인 읽기, 쓰기 등의 액세스 제어를 내부 프로세싱에서 참조 모니터하되, 유저와 서버가 같은 종류의 보안 정책에 의한 보안 레이블일 경우에는 상한 보안레이블을 선택하고, 서로 다른 경우에는 독립적으로 승계하는 보안 모델을 함축한다. 서버엔티티에 대한 알고리즘은 trusted 프로세서 모델[11]의 다중 프로세서 환경과는 달리, 단일 서버엔티티라도 유저엔티티가 보내온 객체에 대하여 허용되지 않는 액세스는 금지시킨다. 따라서, 논문이 추구하는 바는 객체 정보에 대한 원시 액세스 제어와 객체의 서비스 요청에 대한 자격 및 액세스 변형 권한을 종합하여 제어한다.

5.3 객체지향보안시스템과의 비교

객체지향 시스템에 적용된 보안 모델[14]은 서비스를 요청한 객체가 자기 자신일 경우와 이웃 객체인 경우로 구분하여 MLS환경에서 전송제어하며, 내부 프로세싱 제한서비스와 비제한 서비스로 구별하여 쓰기 제어한다. 엔티티와 엔티티 사이의 강제적 레이블에 의한 전송 액세스는 동일하나 객체 지향시스템 보안 정책만을 구현함으로써, 유저 보안정책 구현은 고려되지 못했다. 논문에서는 전술한 바와 같이 서버시스템이 유저 보안 레이블을 지녔다면, 엔티티는 유저환경하에서 유저를 대신하여 액세스 하게되며, 그렇지 않을 시에는 현재 준수하고 있지 않는 환경의 보안 레이블은 비교되지 않은 채로 승계된다. 다른 차이점은 권한 및 특권이나 마킹 등, 실제 환경에서 필요한 기타 보안 요구조건에 대한 대한 액세스 제어를 고려하였다는 점이다.

이상과 같이 관련 연구들을 종합적으로 살펴볼 때, 제안된 알고리즘은 실제 환경을 고려하여 유저와 서버의 2가지 보안 정책의 구현 능력을 지니며, 전송과 내부 프로세싱을 통한 원시 및 서비스 액세스 제어를 포함하고 있다. 모델 관점에서, 두 가지 보안환경으로 부터 발생되는 전송특성과 상한 보안레이블을 승계하며 독립적인 유저 보안정책을 준수하는 내부 프로세싱 특성 이 기존 모델과의 차이로 꼽을 수 있다.

5.4 알고리즘 구현

제안된 알고리즘은 메세지 시스템을 구성하는 각 서버에 대한 액세스제어 메카니즘을 대상으로 한다. 메카니즘의 구현은 서버가 존재하는 컴퓨터 시스템이 분산되어 있는 메세지 시스템 환경에서 컴퓨터 내부에서 서버의 보안 액세스를 제어하는 분산구조의 메세지 보안 메카니즘 구조를 지닐 수도 있고, 메세지시스템 전체에서 발생되는 보안이벤트를 집중하여 관리하는 보안메카니즘 서버가

존재하는 집중구조를 지닐 수도 있다. 후자의 경우, 서버의 모든 보안 액세스는 보안메카니즘 서버의 승인을 득한 후, 처리되는 절차를 거쳐야하므로, 심각한 성능저하를 초래하게 될 것이다. 전자의 경우일 지라도, 각 서버의 보안능력한도, 감사추적정보, 엔티티 식별자 등에 관한 집중구조의 필요성을 피할 수 없다. 디렉토리 서버와 같이 기존에 제안된 집중구조의 서버에 보안관리서버 기능을 추가한다면, 구현상의 중복을 피할 수 있다. 보안관리의 어느 부분을 보안관리 서버에 포함하는 가는 전체 시스템 구현환경에 따라 다를 것이나, 전술한 엔티티의 식별자, 보안처리능력, 감사추적기능은 최소한의 포함 대상이 될 것이다.

알고리즘 구현시 고려할 또다른 사항으로, 기존 컴퓨터 보안 메카니즘과의 중복 또는 분리에 관한 조정이 있을 수 있다. 컴퓨터 보안메카니즘은 일반적으로 원시액세스에 대한 액세스제어를 수행하게 된다. 반면에 제안된 알고리즘은 메세지시스템에서 필요로 하는 원시 액세스 및 응용서비스액세스 제어를 수행하게 된다. 이때, 메세지에 대한 원시 액세스를 컴퓨터 보안 메카니즘의 원시액세스와 동일하게 해석하여 제어함으로써 중복 구현을 피할 수 있으나, 메세지 시스템의 또다른 특수한 보안요구조건에 대한 제어가 필요하게 된다. 만일 메세지 액세스를 컴퓨터 보안메카니즘의 액세스와 동일하게 해석한다면, 메세지에 대한 읽기, 쓰기는 컴퓨터의 read, write커널 시스템 콜과 연결되어 구현되어야 할 것이다. 따라서, 일반적인 read, write 액세스제어를 주관하는 컴퓨터 보안메카니즘과 메세지 시스템을 위한 응용보안메카니즘을 별도로 구현해야하는 이중구조를 지니게 된다. 컴퓨터 보안메카니즘내에 응용서비스보안 메카니즘을 포함하여 구현할 지(신뢰할 수 있는 서버), 분리된 상태에서 상위레벨에 별도로 구현해야 할 지는 구현자의 결정 사항이다. 군용보안 시스템 개발환경은 단일 보안메카니즘 구조를 추구하고 있으나[5], 다중 보안메카니즘의 구현은 분리 구현을 추구하는 추세이다[21].

6. 결 론

본 논문은 메세지 전달시스템의 구체적인 보안정책을 제시하고, 송·수신 엔티티 및 정보 메세지 사이의 전송액세스를 제어하고, 객체 엔티티들과 주체 엔티티 사이의 프로세싱 액세스를 제어하는 메세지 서버엔티티의 참조 모니터 알고리즘을 제안한다. 알고리즘은 유저 보안정책과 메세지 전달시스템의 보안정책을 독립적 또는 종합적으로 준수하며, 보안레이블에 근거한 보안규칙에 의해 원시 및 서비스 액세스가 제어된다. 강제적, 임의적, 마킹, 특권 제어 보안 요구조건은 유저와 메세지 처리시스템의 보안정책을 시스템환경으로 변환한 것이며, 이 요구조건이 만족될 때 메세지는 발신 유저엔티티로부터 유저 보안정책을 준수하는 전달시스템을 경유하여 수신 유저엔티티에게 주어진 보안정책에 위배됨이 없이 전달된다고 할 수 있다. 논문에서 제안하는 알고리즘의 특징은 다음과 같다.

첫째, 서버엔티티는 유저 보안정책을 준수한다. 유저와 서버 보안레이블이 비교될 수 없을 때, 발신 유저엔티티는 신뢰할 수 있는 전송엔티티로 구성된 경로를 거쳐 메세지를 전송할 수 있다.

둘째, 서버엔티티는 유저와 메세지 전달시스템의 보안정책을 종합적으로 준수할 수 있다. 유저와 서버 보안레이블이 비교가능할 때, 메세지 전달시스템은 유저환경과 별도로 높은 보안등급을 부여함으로써 낮은 보안등급 유저로부터의 서비스요청을 거부할 수 있다.

셋째, 서버엔티티의 전송 및 내부 프로세싱 액세스는 참조모니터 된다. 알고리즘은 서버엔티티의 메세지에 대한 모든 액세스를 제어한다. 이러한 액세스는 원시 및 서비스를 포함하여, 유저 및 서버 보안정책을 모두 적용한다.

넷째, 보안정책은 다중 보안레이블에 의해 구현된다.

주체와 객체에 부여된 강제적, 임의적, 마킹, 특권의 다중 보안레이블에 근거하여 보안규칙 위배 여부가 결정된다.

알고리즘은 서버엔티티의 보안메카니즘의 액세스제어관점에서 제안되었다. 향후, 구현관점에서 볼때 정형화된 모델링, 메세지의 안전한 end-to-end 정보흐름, 보안구조 및 설계 연구가 추가로 필요하다고 생각된다. 아울러, 응용분야측면에서의 연속된 보안정책 및 독립된 여러 유저환경에서의 보안정책 구현 연구도 병행되어야 한다고 사료된다.

참 고 문 헌

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

[2] CCITT, Data Communication Networks Directory, Recommendations X.509, Nov. 1988.

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

[4] ISO/IEC, Information Technology-Open Systems Intercornection-Security Framewoks in Open Systems-Part3 : Access Control, Jun. 1992.

[5] Department of Defence Computer Security Center, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-005, Version 1, Jul. 1987.

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

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

[8] Clark D.D., D.R. Wilson, "A Comparision of Commercial and Military Computer Security Policies," Proceeding of the 1987 Symposium on Security and Privacy, Oakland,CA,IEEE Computer Society Press, pp. 184-194, Apr. 1987.

[9] Mclean J., "Reasoning about Security Models", Proceeding of the 1987 Symposium on Secuity and Privacy, Oakland,CA,IEEE Computer Society Press, pp. 123-131, Apr. 1987.

[10] Landwehr J.,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.

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

[12] Sandhu, R.S., "The Typed Access Access Matrix Model", Proceedings of the Symposium on Research in Security and Privacy, Oakland, CA, IEEE Computer Society Press, pp. 122-136, May 1992.

[13] Sandhu, R.S., "Transaction Control Expressions for Seperation of Duties", Proceeding of the 4th Aerospace Computer Securtiy Applications Conference, Orlando, FL,pp.20-46, May 1989.

[14] Bertinto E., Samarati P., Jajodia S., "High Assurance Discretionary Access Control for Object Bases", Proceeding of the first Conference on Computer and Communication Securtiy, Fairfax, VA, ACM SIGSAC, pp. 144-150, Nov. 1993.

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

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

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

[18] Graubart T.D., "On the Need for a Third Form of Access Control", Proceeding of the 13th National Computer Security Conference, Baltimore, MD,pp. 296-303, Oct. 1989.

[19] McCollum C.J.,J.R. Messing, and L. Notargiacomo, "Beyond the Pale of MAC and DAC-Defining New Forms of Access Control", Proceeding of the 1989 Symposium on Security and Privacy, Oakland, CA, IEEE Computer Society Press, pp. 23-30, May 1990.

[20] Gligor V.D., "Unix without the Super user", 1987 Summer USENIX Conference, Phonix, Arizona, pp. 243-256, Jun. 1987.

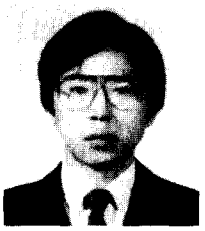
[21] Abrams M.D, "Renewed Understanding of Control Policies", Proceeding of the 16th National Compuer Security Conference, Baltimore, MD, pp. 87-96, Oct. 1993.

[22] Gosselin M. J., "Message Handling Systems(X.400) Threats, Vulnerabilities, and Countermeasures", Proceeding of the 13th National Compuer Security Conference, Baltimore, MD, pp. 226-235, Oct. 1993.

[23] Muftic S. A Patel, P. *Sanders, Security Architecture for Open Distributed Systems*, John Wiley & Sons, 1993.

[24] Kim D.K.,S.W.Kim, "A Security Model for Store and Forward Message Handling System", Technical Report of IEICE, Vol. 93, No. 295, IEICE, Japan, Oct. 1993.

□ 著者紹介



김 석 우

한국 항공 대학 통신공학과(학사)
뉴저지 공과대학 전자계산학과(석사)
아주대학교 컴퓨터공학과 박사과정
삼성전자 HP 사업본부 근무, AT & T Bell lab. 방문 연구원
현재 한국전자통신연구소 실장

※ 주관심분야 : 컴퓨터 Security, 정보통신 Security

김 동 규

서울대학교 공과대학 졸업(학사)
서울대학교 자연과학대학원 졸업(석사)
미국 Kansas 주립대 대학원 졸업(전산학 박사, 정보통신 전공)
미국 Kansas 주립대 전산학과 교수
1973. 3 - 현재 아주대학교 컴퓨터공학과 교수
저서 : 데이타 통신시스템, 회중당, 1986년
컴퓨터 통신 네트워크, 상조사, 1988년
한국통신학회 상임이사, 개방형 컴퓨터통신 연구회(OSIA) 이사,
한국 ISO/TC97/SC6/SC21/SC27 전문기술 연구위원,
한국통신정보보호학회 부회장
※ 주관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링,
정보통신 Security, 분산처리 시스템