안전한 운영 체제를 위한 보안 요소 설계

윤 이중, 홍 주영, 김석우, 김대호
한국 전자 통신 연구소

The Design of the Security Elements for Secure Operating System

E-Joong Yoon, Joo-Young Hong, Seok-Woo Kim, Dae-Ho Kim
Electronics and Telecommunications Research Institute

요 약

정보 처리가 자동화 됨에 따라, 종래의 문서 처리에서 적용되었던 보안 개념을 지원하는 안전한 컴퓨터 시스템에 대한 요구가 증가되고 있다. 본 연구에서는 안전한 컴퓨터 시스템을 수학적으로 정의하고 증명한 BLP 모델을 고찰하고, 그 각 요소들을 실제 시스템에 적용시 해석 방법과 시스템 요소들과의 대응 관계 및 액세스 제어 메카니즘을 제시하고자 한다.

1. 서 론

정보의 보호 측면에서 수작업 방식은 오랜 역사를 통하여 문제점이 보완되었으며 적어도 표면적으로는 정보보호에 문제가 없는 것으로 인식되고 있다. 그러나 컴퓨터 시스템을 이용한 정보처리가 이루어지게 되면서 정보의 작성, 편집, 변경등은 상당히 편리해지고 단순해졌으나 열람, 분배, 변경, 보관등에 있어서 여러가지 보안상 어려움이 나타났다. 따라서 정보보호개념을 확실히 지원해 주어야 할 안전한 컴퓨터 시스템 (secure computer system)의 등장을 절실히 필요하게 되었다[1].

컴퓨터 시스템에서의 안전성 (security) 이란 의미는 각 조직의 특수한 환경, 요구조건에 따라 달

라질 수 있다. 이는 결국 안전성의 의미는 각 조직의 보안정책 (security policy)에 의해 정의되어지는 것이지 모든 환경에 일률적으로 적용되어지는 의미가 아니라는 것이다.

현재 가장 대표적인 보안 정책은 정보의 불법 유출방지와 정보의 불법 변경방지로 크게 나눌수 있으며, 이들 보안 정책들을 수학적으로 정의하고 검증한 보안 정책 모델 (security policy model)이 발표되었다. 정보의 불법 유출 방지 정책의 가장 대표적인 보안 정책 모델로 Bell-LaPadula (BLP)모델이 있다[3, 10].

이러한 보안 정책들을 목표로 하는 안전한 컴퓨터 시스템에 관련된 사람들은 시스템 사용자, 개발자, 구매자의 세가지 부류로 나눌 수 있고 이들은 다음과 같은 요구 사항을 갖는다. 첫째, 컴퓨터 시스템에 정보를 저장하여 사용하는 시스템 사용자는 자신이 사용하는 컴퓨터 시스템의 안전성 수준을 측정 할 수 있는 척도를 필요로 한다. 둘째, 안전한 컴퓨터를 개발하는 개발자는 구매자의 보안 요구를 만족 시킬 수 있는 시스템 개발을 위한 평가서가 필요하다. 세째, 구매자는 그들의 보안 요구 사항을 명시 할 수 있는 기준서가 필요하다. 이러한 요구 사항을 기술한 문서들로 1983년 미국방성의 TCSEC, 1987년 영국의 Green Book, 1990년 독일을 중심으로한 유럽의 ITSEC, 1989년 카나다 Orange Book등이 있다.

안전한 컴퓨터시스템을 개발하는 절차는 첫째, 보안 정책의 선정 단계 둘째, 보안모델의 선정 단계 세째, 모델의 각 요소들을 대상 시스템 요소로 해석 하는 단계 네째, 자국의 평가 기준서의 요구사항에 따른 개발 단계 등으로 나눌 수 있다[6, 7].

본 논문에서는 BLP 모델을 채택한 UNIX 계열의 안전한 컴퓨터 개발시 모델의 각 요소들을 시스템 환경에 맞게 해석하는 단계에서의 필수적인 고려 사항 및 대응 관계을 제시하고, TCB(Trusted Computing Base)의 복잡도가 최소화 되어야 한다는 TCSEC의 요구를 만족하는 보안 관리자에 대하여 기술한다. 2장에서 BLP모델을 요약하며, 3장에서 시스템에서의 BLP모델 해석에 대하여 기술하고 4장에서 결론과 추후 연구과제등을 기술하였다.

2. BLP 모델의 고찰

보안정책에 대한 여러가지 모델들이 제안되었고 BLP 모델도 그중의 하나이다. BLP모델은 시스템 요소와 시스템의 상태를 변경시키는 규칙 (rule)들을 정형적으로 정의한 상태전이 (state transition) 모델이다[4]. 이 모델은 정보의 불법 유출 방지를 보안정책으로 채택한 안전한 시스템의 설계를 위한 기준이 되어지고 있으며 이는 TCSEC(Trusted Computer System Evaluation Criteria)에서 보안정책의 기본으로 사용되고 있다.

2.1. 시스템 상태 (system state)

시스템상태V 는 다음과 같이 정의된다.

V = (b x M x f x H)

1) B는 현재 액세스 집합(current access set)으로 이는 다음과 같이 정의 된다.

b = (S x O x A) S : 주체의 집합

O : 객체의 집합

A : 시스템에서 정의된 액세스 모드의 집합

즉 b는 임의 주체가 임의 객체에 대해 DAC와 MAC의 조건을 만족한 후 취득하여 현재 가지고 있는 액세스 모드를 의미한다.

2) M은 액세스 매트릭스를 나타내며 이는 임의 주체(Si)가 임의 객체(Oj)에 대하여 소유한 액세스 모드를 그 원소로 하며 이들은 객체의 소유자에 의해 결정되고 다음과 같은 조건을 갖는다.

$Mij \in A$

3) H는 트리 형태를 갖는 객체 구조를 나타낸다.

4) f는 세가지 보안 함수로 이루어진다.

fs : 주체의 최대 보안 등급

fo : 객체의 보안 등급

fc : 주체의 현재 보안 등급

여기서 fs와 fc의 관계는 항상 $fs \geq fc$ 를 유지하여야 한다.

2.2. 상태 전이 (state transition)

시스템의 상태 전이는 주체에 의해 요구되어지는 규칙 (rule)들에 의해 발생된다.

규칙 ρ 는 다음과 같이 정의된다.

$\rho = R \times V \rightarrow D \times V$ $\quad R \times V$: request - state pair

$D \times V$: decision - state pair

$D = \{yes, no, ?, error\}$

$\{\rho 1, \ldots, \rho s\}$를 규칙의 집합이라하고 상태 전이의 집합을 W라 하면 $Dm \neq ?, Dm \neq error$이고 유일한 $i(1 \leq i \leq s)$에 대하여 $(Dm, V^*) = \rho i\,(Rk, V)$ 일때 상태 전이의 집합은 다음과 같이 정의 된다. $\{Rk, Dm, V^*, V) \in W(w)$ $\quad Rk \in R$

$Dk \in D$

$V^* \in V$

2.3 모델 공리

BLP모델에서는 시스템이 안전한 상태를 유지하기위해 지켜야 하는 세가지 특성이 있다.

2.3.1. Simple Security Property(ss-property)

시스템 상태 $v = (b, M, f, H)$에서 $(s, o, x) \in b$는 다음과 같을때 ss-property를 만족한다고 한다

i) $x = e$ or a

ii) $x = r$ or w and $fs(s) \geq fo(o)$

2.3.2. Star Property (*-Property)

시스템 상태 $V = (b, M, f, H)$는 다음 조건을 만족할 때 *- Property를 만족한다고 한다.

i) $x = a \Rightarrow fc(s) \leq fo(o)$

ii) $x = w \Rightarrow fc(s) = fo(o)$

iii) $x = r \Rightarrow fc(s) \geq fo(o)$

* - Property는 보안등급이 높은 객체에서 보안등급이 낮은 객체로의 허가 되지 않은 정보의 흐름을 방지하는 것이 목적이며 이는 신뢰할수 없는 주체에 대하여 적용된다.

2.3.3. Discretionary Property(ds-Property)

시스템 상태 $V = (b, M, f, H)$는 $(Si, Oj, X) \in b$ 가 다음 조건을 만족할 때 ds- property를 만족한다고 한다.

i) $x \in Mij$

3. BLP 모델의 해석

3.1. 시스템 상태 해석

시스템 상태 V는 S x O x A, M, f, H로 이루어져 있고 이들 각 요소들에 대한 해석은 다음과 같다.

3.1.1. 주체 (S)

시스템에서 프로세스는 유일한 주체이다. 프로세스는 객체를 생성, 삭제하고, 액세스 메트릭스내의 액세스모드와 현재 액세스 집합의 내용을 변경시킨다. 객체에 대한 프로세스의 모든 액세스 취득 행위는 세가지 보안 특성을 만족할 경우만 허용된다. 프로세스의 보안 등급은 사용자의 보안 등급을 계승하며 이는 주체 최대 보안 등급과 현재 보안 등급으로 구성된다.

3.1.2. 객체 (O)

시스템에서 객체로 인식되어 지는 것은 사용자가 생성하는 화일, 디렉토리와 특수한 화일인 디바이스등이 있으며 그이외에 파이프, 메세지 큐, 공유 메모리등이 있다. 이들 객체의 특성은 모델의 액세스 모드를 해석하는데 중요한 고려 사항이 된다. 즉 이들의 특성에 따라 모델의 액세스 모드는 의미를 달리한다. 기존 UNIX 계열의 시스템에서 /tmp, /usr/spool, /dev/null등은 보안 등급이 다른 객체들이 다루어지는 디렉토리이기 때문에 MAC의 적용에서 문제가 발생한다. 이의 해결을 위하여 /tmp 문제는 사용자에는 보여지지 않는 서브 디렉토리를 이용하는 방법이 제시되었고, /usr/spool과 /dev/null은 wildcard(*)보안 등급을 이용하여 해결하는 방법이 제시되었다.

BLP 모델	e	r	re	a	w
화일	-	r	x	w	rw
디렉토리	-	r or x	(x)	w	rw
디바이스	-	r	x	w	rw

<그림 1 > Secure Xenis의 액세스 모드 해석

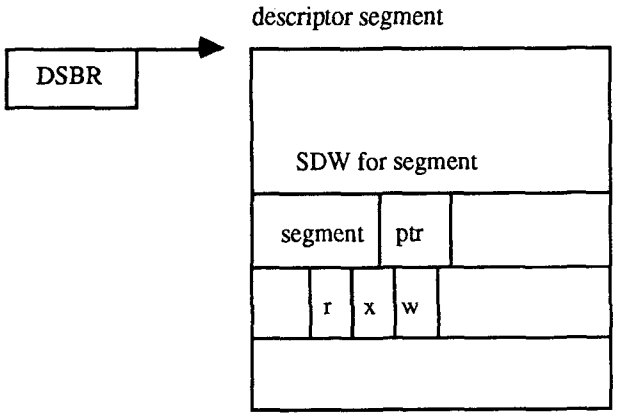
3.1.3. 액세스 모드 집합 (A)

BLP 모델에서의 액세스 모드는 read, append, execute, write의 네가지 종류이다. 이들 BLP모델

의 액세스모드와 실제 시스템에서의 액세스모드는 그 의미가 1 : 1로 매핑되지 않으며 이는 객체의 특성 때문이다. Secure Xenix에서의 객체들에 대한 모델의 액세스 모드 해석은 <그림 1>과 같다.

3.1.4. 현재 액세스 집합(b)

현재 액세스 집합 b는 임의 주체가 임의 객체에 대하여 DAC와 MAC에 의해 허가 받은 액세스모드를 의미한다. Secure MULTICS에서는 각 프로세스 별로 그 정보를 관리하며 이를 위하여 DSBR(Descriptor Segment Base Register), TPR(Temporary Pointer Register), SDW(Segement Descriptor Word)의 세가지 자료 구조<그림 2>가 사용된다.



<그림 2> Secure MULTICS에서의 b에 대한 자료 구조

3.1.5. 액세스 매트릭스 (M)

시스템에서 개인 단위로 DAC의 제어를 가능케 하도록 하기위해 ACL(Access Control List)이 도입되었고 ACL을 사용하는 시스템은 secure Xenix, secure MULTICS등이 있다. ACL은 기존 UNIX에서사용하는 SGP(Self/Group/Public) 비트의 내용을 포함 할 수 있어야 하며 그의 구성 은 (uid, gid, x)의 리스트로 구성된다. SGP의 내용을 ACL로 표현 하면 다음과 같다[9].

{(as), (ag), (ap)} = {(us, *, as), (*, gg, ag), (*, *, ap)}

3.1.6 보안 함수(f)

보안 함수는 주체의 최대 보안 등급, 현재 보안 등급의 할당과 객체의 보안 등급 할당을 담당한다. 주체의 최대 보안 등급은 시스템 보안 담당자가 할당해 주며 이는 시스템 최고 등급과 시스

템 최저 등급 사이에 있어야 한다. 주체의 현재 보안 등급은 주체 최대 보안 등급과 시스템 최저 보안 등급 사이에 있어야 하며 현재 보안 등급에 영향을 주는 또다른 영향은 터미날 최대 보안 등급이 있다.

3.2. 상태 전이

시스템이 안전하다는 것은 결국 b, M, f ,H에 대한 변화가 세가지 특성을 만족한다는 것을 의미한다. 사용자가 시스템 상태를 변경 할 수 있는 방법은 시스템 호출을 사용하는 것이다. 이들 시스템 호출은 네가지 범주로 이루어진다.

3.2.1. 현재 액세스 집합의 변경 (b)

-get access

-release access

b에 대한 변경은 주체가 객체에 대한 액세스 모드를 요청하는 시스템 호출을 사용했을 때 발생한다. 요청한 액세스 모드를 허가 받기위해서는 DAC와 MAC의 조건을 모두 통과하여야 한다.이때 허용된 액세스 모드는 b의 요소가 된다. b에대한 변경을 처리하기 위해 setmac()와 getmac()의 두 가지 시스템 호출을 생성하여야 한다.

3.2.2. 액세스 매트릭스의 변경(M)

- get access permission

- rescind access permission

BLP 모델에서 액세스 매트릭스의 형태에 대한 특별한 요구는 없다. 기존의 UNIX에서 사용하고 있는 SGP로 표현되는 정보를 포함할 수 있는 ACL을 도입 할 경우 DAC를 위해 생성될 시스템 호출들은 다음과 같다.

- ACL의 생성과 삭제를위한 mkacl(), delacl()

- ACL에 엔트리 추가와 삭제를 위한 addacl(), delacl()

- ACL의 엔트리 내용 변경과 검색을 위한 chacl(), getacl()

3.2.3. 계층 구조의 변경(H)

- create Oj

- delete Oj

객체의 생성시에 문제가 되어 지는 것은 객체의 계층구조 사이의 보안 등급 할당이다. BLP모델에서 객체 생성시 상위 객체(Oi)의 보안등급을 생성되는 객체(Oj)의 보안 등급이 우선 (fo(Oi) ≤ fo(Oj)) 하여야 할 것을 요구한다. 이들 객체들 간의 보안 등급의 제약 조건을 유지하기 어려운 디렉토리들에 대하여 그 종류와 해결 방안을 3.1.2절에서 기술 하였다.

3.2.4. 보안 등급 함수의 변경(f)

- change object security lebel

- change current security lebel

주체의 최대 보안 등급은 시스템 보안 관리자에 의해서 주어지며 주체의 현재 보안 등급은 최대 보안 등급과 시스템 최저 보안 등급 사이에존재해야 하며 만약 단말기에 할당된 보안 등급이 있다면 현재 보안 등급은 이를 우선할수 없다. 현재 보안 등급의 변경은 또한 현재 액세스 집합을 나타내는 b의 요소인 액세스 모드에 대하여 변경시 위반 사항이 없는 범위에서 행해져야한다. 객체의 보안 등급 변경은 상위 객체의 보안 등급을 우선해야하며 또한 b의 요소인 액세스 모드 들이 보안 등급이 변한 후에도 유지되어 지는 범위에서 변경 되어야 한다.

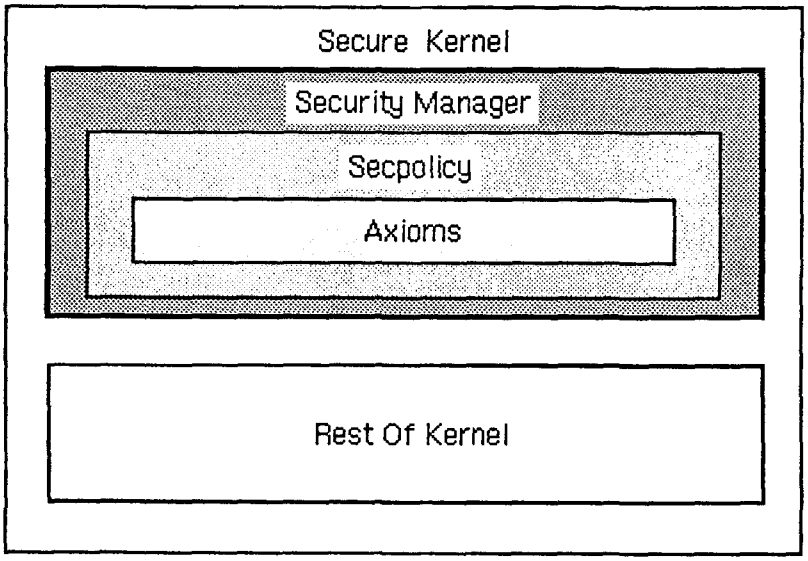
3.3 액세스 제어 메카니즘

기존 UNIX 계열의 커널 구조는 모듈화의 약점으로 인하여 TCSEC 기준으로 B3급 이상의 시스템을 구성하지 못한다[8]. 최근 기존 UNIX의 호환성을 지니면서 커널 구조가 잘 모듈화되어 있고 또한 계층적 구조를 지니는 시스템 들이 개발되고 있다. 이들 시스템들은 TCSEC 기준으로 B3급의 요구사항인 복잡도의 최소화, 계층화, 추상화를 만족 시키는 TCB를 구성 할 수 있다. 이런 시스템에서 보안 검사를 전담 할 수 있는 참조 모니터 개념의 보안 관리자<그림 3> 를 설계 할 수 있다. 이 보안 관리자는 두개의 모듈로 구성되며 시스템이 유지해야하는 세가지 보안 특성 들로 이루어진 하위모듈과 각 시스템 호출에 적용 되어져야 하는 보안 특성들의 집합과 보안 검사를 위해서 행해지는 부수적 기능들로 이루어진 상위 모듈로 구성된다.

4. 결 론

본 논문에서는 안전한 컴퓨터 운영 체제의 개발 단계중 보안 모델을 시스템 요소로 해석하는 단계에서 모델요소와 시스템 요소와의 매핑 관계와 시스템이 유지하여야 하는 보안 특성의 적용시 기존의 처리 방법을 변경해야하는 객체들을 기술하였다. 또한 액세스 제어 메카니즘 을 위해

설계된 보안 관리자로 인하여 기존 모듈에 대한 최소한의 변경만으로 보안 기능을 첨가 할 수 있으며, TCSEC의 TCB(Trusted Computing Base)는 복잡도가 최소화 되어야한다는 요구조건을 만족한다. 특히 SecPolicy와 SecAxiom의 분리는 보안 정책의 변경시 최소의 경비로 시스템을 재구성할 수 있다는 장점을 지니고 있다. 안전한 시스템 개발시 적용되어야 할 정형화 개발과정에 대한 연구와 기존 UNIX의 보안 등급을 향상 시키기 위한 방안이 계속 연구되어야 한다.



<그림 3> 보안 관리자 구성도

참 고 문 헌

[1] C.E. Landwehr, "Formal Models for Computer Security", ACM Computing surveys, Vol. 13, No. 3, September 1981.

[2] D.D. Clark, "A Comparison of Commercial and Military Computer Security Policies", Proceedings of IEEE Symposium on Security and Privacy, April 1987.

[3] D.E. Bell, "Concerning Modeling of Computer Securty", Proceedings of IEEE Symposium on Security and Privacy, April 1988.

[4] D. E. Bell, "Secure Computer System : A Refinement of The Mathematical Model",MITRE, ESDTR-73-278, Vol.3, April 1974.

[5] DoD NCSC, Trusted Computer System Evaluation Criteria, DoD 5200. 28-STD, NCSC, December 1985.

[6] J.A. Goguen and J. Meseguer, "Security Policies and Security Models", Proceedings of IEEE Symposium on Security and Privacy, April 1982.

[7] M. Gasser, Building A Secure Computer System, Van Nostrand Reinhols Company Inc., 1988.

[8] G.L. Grenier, "Policy vs Mechanisms in the Secure TUNIS Operating System", proceedings IEEE Symposium on Security and Privacy, May 1989.

[9] Mark Funkenhauser, "B1 TUNIS : A Kernel for a Secure UNIX System" Canadian Com puter Security Conference, 1989.

[10] Biba, K.J. "Integrity Considerations for Secure Computer System"MTR-2997, MITRE Corp., Bedford, Mass., July 1985.