프로세스 신뢰도에 기반한 확장된 BLP 보안 모델과 아키텍처 설계

강정민°, 신욱, 박춘구, 이형효, 이동익
광주과학기술원 정보통신공학과
{jmkang, sunihill, cgpark}@geguri.kjist.ac.kr
{hlee, dilee}@kjist.ac.kr

Extended BLP Security Model based on Process Reliability and Architecture Design

Jung-Min Kang°, Wook Shin, Chun-Goo Park, Hyung-hyo Lee, Dong-Ik Lee
Department of Information and Communications, K-JIST

요 약

안전한 운영체제를 개발하기 위해 제안된 모델중 대표적인 BLP(Bell & LaPadula) 모델은 주체(사용자)의 보안등급이 접근주체인 프로세스에 그대로 상속됨으로서 악의적인 프로세스에 의한 정보의 흐름, 변조, 누출 등의 위협을 고려하지 않는 단점을 지니고 있다. 본 논문에서는 프로세스를 신뢰영역과 비 신뢰영역으로 구분하고 악의적인 행위를 유발할 수 있는 프로세스들의 접근을 강력히 통제하는 프로세스 기반의 확장된 BLP 모델을 제안하고 시스템에 적용을 위한 아키텍처를 설계한다.

1. 서론

최근 정보화 역기능에 관한 관심이 심화되고 있어 원천적인 정보보호에 대한 필요성이 제기되고 있다. 안전한 운영체제의 개발은 이를 위한 필수적인 과제라 할 수 있으며, 지금까지 개발된 안전한 운영체제 관련연구의 대표적인 사례를 살펴보면 [표 1]과 같다. 이들은 TCSEC[1] B급 이상의 요구사항을 만족시키기 위해 객체에 포함된 정보의 기밀성(sensitivity)과 주체에게 부여된 신원허가(clearance)를 기반으로 하여 주체의 객체에 대한 접근을 통제하는 강제 접근통제(MAC) 규칙을 적용하며, BLP 모델을 채택하고 있다. 하지만 이제까지의 연구 사례들을 검토해보면 BLP 모델을 적용함에 있어서 사용자의 보안등급을 프로세스에 그대로 상속하고 있음을 알 수 있다. 이러한 접근방법의 문제점은 프로세스를 전적으로 신뢰할 수 없다는 것에서 기인한다. 즉, 사용자의 신용등급과 권한허용 범위를 오류가 내재되어 있거나 의도적으로 수정된 악의적인(malicious)프로세스에게 그대로 상속할 경우, 시스템 안전성이 파괴될 가능성이 있다. 이는 BLP 모델이 *접근 주체를 정의함에 있어서 시스템 사용자와 실제* 그 접근을 대행하는 프로세스를 동일시 하도록 단순하게 정의하고 있기 때문이며, 따라서 사용자와 프로세스간 신뢰관계를 모델에 도입함으로써 해결 가능하다. 본 논문에서는 보다 강력한 접근통제를 위해 프로세스 신뢰도에 기반한 확장된 BLP 모델을 제안하고 시스템에 적용을 위한 아키텍처를 설계한다. 본 논문의 구성은 다음과 같다. 2장에서는 기존 BLP 모델의 개요와 문제점을 기술하며, 3장에서는 단점들을 해결할 수 있는 제안된 모델에 대해, 4장에서는 본 논문의 결론과 향후 연구과제에 대해 논한다.

	R & D	기관/장소
마이크로 커널기반	Synergy DTOS	NSA,NIST,DISA,ARPA공동추진
	Fluke/Flask	Utah 대학주관
	EROS	TymShare Inc.
통합커널기반	MLS-L4리눅스	한서대학교
	SecuRos	ETRI
	RSBAC	독일 Hamburg대학
	Medusa	슬로바키아
	seLinux	NSA

표 1 안전한 운영체제 개발 현황

2. BLP 모델의 개요와 문제점

BLP 모델의 접근통제를 위한 메커니즘은 다음과 같다. 첫째, DAC 정책을 적용하여 접근행렬에 저장되어 있는 주체의 객체에 대한 접근 권한과 요청된 접근 권한이 일치하는가를 확인하는 ds-property검사를 한다. 다음, 강제 접근통제(MAC)를 적용하여 주체와 객체에 부여된 보안등급간 ss-property와 *-property 검사를 수행한다[1][4][5]. 이는 다음과 같은 알고리즘으로 요약된다[그림 1]. BLP 모델의 기본철학은 현재 상태에서 다음 상태로의 변경이 있을 때, 위에서 언급한 성질들이 만족되면 시스템의 보안이 유지된다는 것이다. 하지만 다음과 같은 문제점들이 지적될 수 있다[2].

① 정보의 무결성(Integrity)을 배제하고 기밀성만을 고려

```
접근허가결정검사 (s, o, m) {
    return ( ds_property check;      // true or false
          && ss_property check;  // true or false
          && *-property check; ) // true or false }
```

[그림 1] BLP 모델의 접근허가결정 알고리즘

한다. 즉 임의의 프로세스에 의해 정보가 불법적으로 변경(write)될 수 있는 가능성을 고려하지 않고 주체(사용자)에 의한 정보의 접근통제만을 고려한다.

② 식별(Identification)과 인증(Authentication)과정을 거친 인가된 사용자가 악의적인 프로세스(실질적 접근주체)를 실행함으로서 중요한 정보에 접근(read)할 수 있는 것은 정보의 기밀성을 위배하는 것이다.

③ 접근통제의 관리적 측면을 고려하지 않는다.

④ 공모에 의해 one bit information flow 같은 Covert channel이 존재 할 수 있다.

문제점 ①, ②의 근본적인 원인은 사용자와 실제 시스템의 접근주체인 프로세스를 동일시 함으로써 생긴다. 이제까지의 안전한 운영체제 연구 사례들은 BLP 모델을 적용함에 있어서 사용자의 보안등급을 프로세스에 그대로 상속함으로 BLP 모델의 근본적인 문제점을 해결하지 못하고 있다. 이 논문에서는 위의 ①, ②에 관해서 고려한다.

3. 프로세스 신뢰도에 기반한 확장된 BLP 모델

BLP 모델을 적용하는 대부분의 시스템에서 사용자는 id/password를 이용하여 식별과 인증절차를 수행하고, 이 과정이 끝나면 허가(clearance)와 부서(category)정보를 입력한다. 여기서 입력한 허가, 부서 정보는 시스템 사용을 위해 그 사용자가 수행하는 모든 프로세스에게 상속되어 접근 통제시 주체의 권한 정보로 이용된다. 그러나 현존하는 프로그램의 버그, 악성 프로그램의 예에서 보듯 모든 프로세스가 정확히 동작하여 시스템에 위해를 가하지 않으리라는 보장을 할 수 없으므로 사용자 접근을 대행하는 프로세스 자체의 신뢰성은 전체 시스템의 보안과 밀접한 관련이 있다고 할 수 있다. 본 논문에서는 이러한 사실을 수용하기 위해 기존의 BLP 접근통제 모델을 확장하여, 다음과 같이 프로세스 신뢰도에 기반한 확장된 BLP 접근통제 모델을 제안한다.

[정의 1] 구성 요소

- S : 사용자들의 보안등급(Clearance)
- P : 프로세스들의 집합
- O : 객체들의 집합(파일, 디렉토리, 장치 등)
- A : 접근모드의 집합 = { r, w, a, e }
  r: read_only, w: read_write,
  a: write_only(append),
  e: neither read nor write(execute).

[정의 2] 시스템의 상태

V = (B, M, F)로 시스템의 상태를 정의한다.

- B = (S, P, O, A) : 현재의 접근 권한 집합으로서 원소 b (∈ B) 는 (s, p, o, a)로 구성되며, 사용자 s 가 프로세스 p를 실행해서 객체 o 에 대하여 a 모드로 현재 접근함을 나타낸다.
- M : 접근행렬로서 사용자가 객체에 대해 실행할 수 있는 접근모드를 나타낸다.
- F : (f_s, f_c, f_p, f_o) 형태의 등급 및 신뢰성 할당함수
  $f_s(s)$: 사용자 s 의 최고 보안등급(clearance)
  $f_c(s)$: 사용자 s 의 현재 보안등급
  $f_p(p)$: 활성화된 프로세스의 신뢰여부(True/False)
  $f_o(o)$: 객체 o 의 보안등급(classification)
  $\forall s \in S, f_s(s) \geq f_c(s)$ 이다.

[정의 3] 안전한 상태

확장된 BLP 모델은 시스템이 안전하기 위해서 다음과 같은 성질들을 만족해야 한다.

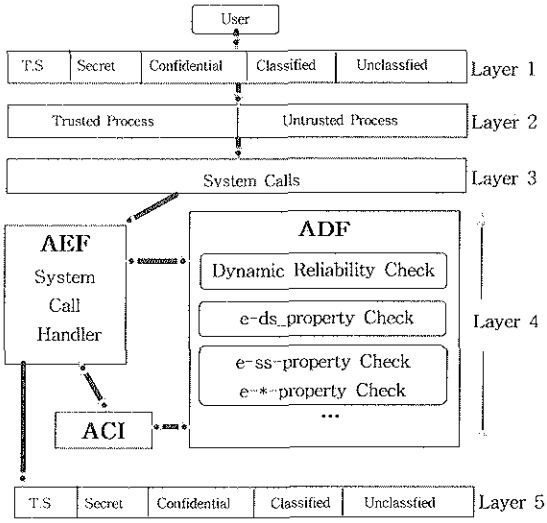
① Extended Simple Security property(e-ss-property)
if mode=r or w(∈M[s,o]),
$f_p(p)$=true and $f_c(s) \geq f_o(o)$. (no read-up).

② Extended Star-property(e-*-property)
if mode= a(∈M[s,o]), $f_p(p)$=true and $f_c(s) \leq f_o(o)$.
if mode= w(∈M[s,o]), $f_p(p)$=true and $f_c(s) = f_o(o)$.
if mode= r(∈M[s,o]), $f_p(p)$=true and $f_c(s) \geq f_o(o)$.
(no write-down).

③ Extended ds-property(e-discretionary security)
if (s, p, o, a) ∈ B, $f_p(p)$=true and m ∈ M[s,o].
if (s, p, o, a) ∈ B, $f_p(p)$=false and
$f_o(o)$ = Unclassified and m ∈ M[s,o].

다음은 확장된 BLP 모델을 시스템에 적용하기 위한 아키텍처 이다[그림 2].

- Layer 1: 사용자 보안 등급(Clearance)
- Layer 2: 정적 신뢰도 검사
- Layer 3: 시스템에 접근하기 위한 시스템 호출



[그림 2] 프로세스 신뢰도 기반의 접근 통제 아키텍처

- Layer 4: 접근통제를 위한 참조모니터
  - AEF(Access Enforcement Facility): 접근제어 집행부
  - ACI(Access Control Information): 접근제어 정보
  - ADF(Access Decision Facility): 접근 결정부
- Layer 5: 객체들의 보안등급(Classification)
  - T.S ~ Classified: 조직에서 반드시 보호해야 되는 중요(Sensitive) 정보
  - Unclassified: 조직에서 게시판 정보 같은 공유될 수 있는 정보

사용자는 시스템 관리자에 의해 부여된 id/password 및 clearance/category정보를 입력함으로써 시스템에 로그인 하게된다(Layer 1). Layer 2에서 인가된 사용자가 객체에 접근하기 위해 실행하는 프로세스는 정적 신뢰성 정책에 의해 분류된 신뢰적 또는 비 신뢰적인 프로세스이다. 여기서 정적이라 함은 시스템 관리자가 조직원들과의 상의를 통해 결정하는 프로세스 신뢰도 평가를 의미하며 다음과 같은 신뢰도 평가 기준을 둘 수 있다.

● 정적 신뢰도 결정 기준
- 기존에 알려진 해킹관련 프로그램들
  예: scan도구, password crack도구 등
- 일반 사용자들이 생성한 검증이 안된 프로그램들

접근 주체가 비 신뢰적인 프로세스로 판명되면 이 주체가 접근할 수 있는 객체는 참조모니터에 의해 Unclassified level의 객체로 제한이 된다. 이는 인가된 사용자가 실행하는 모든 프로세스에 의해 객체의 변경(write)을 허용함으로써 정보의 무결성을 위배할 수 있는 기존의 BLP 모델의 단점을 극복하기 위함이다. 만일 인가된 사용자가 Trusted 프로세스를 실행해서 객체 접근을 요구한다면 우선적으로 ADF의 Dynamic Reliability Check(DRC) 모듈은 ACI의 프로세스 패턴정보를 이용해 동적으로 프로세스의 신뢰성을 검사한다. 이는 비록 Trusted 프로세스 일지라도 일정한 패턴을 가진 불법적인 행위가 시스템에 유해한 행위를 할 수 있기 때문이다. 다음은 동적 신뢰도 검사 기준이 될 수 있는 항목들이다.

● 동적 신뢰도 결정 기준
- OS보안에 관련된 취약한 utility또는 서비스들과 관련된 행위패턴[3]
  예: backdoor 용으로 주로 교체되는 프로그램들(login, su, telnet, in.telnetd, ftp, ls, ps, netstat, ifconfig, *find, du, df, inetd, sync, libc, syslogd* 등)
- 위험한 함수를 사용하는 프로그램들의 행위들
  예: 버퍼경계를 체크하지 않는 알려진 함수들을 사용하는 프로그램들(strcpy, strcat, getwd, gets, fscanf, scanf, realpath, sprintf 등)

DRC 모듈을 통과한 Trusted 프로세스는 확장된 BLP 모델을 따른 e-ds-property, e-ss-property 와 e-*-property 검사를 순차적으로 거치게 된다. 따라서 확장된 BLP 모델을 적용한 시스템은 인가되고, 신뢰적인 프로세스의 객체 접근(read)을 보장하여 정보의 기밀성을 유지하며, 비 신뢰적인 프로세스의 접근을 Unclassified 객체로 제한하여 중요 정보의 불법변경을 최대한 억제하므로 정보의 무결성을 보장한다. [그림 3]은 제안된 모델에서의 AEF의 접근결정을 위한 알고리즘이다.

```
AEF(s, p, o ,m) {
boolean t, a1, a2, a3;
 t = Dynamic Reliability Check(p);
 if(t==true) {
    a1= e-ds_property check(s,p,o,m);  // true or false
    a2= e-ss_property check(s,p,o,m);  // true or false
    a2= e-*-property check(s,p,o,m);  // true or false
    return (a1 && a2 && a3); }
 else { return(e-ds_property check()); }
}
```

[그림 3] 확장된 BLP 모델에서의 AEF 알고리즘

4. 결론 및 향후 연구과제

실제 사용자의 권한이 시스템 내 접근통제 시스템에서는 접근 주체 설정을 위해 프로세스로 전이됨을 고려할 때, 악의적인 프로세스의 통제는 필수적인 과제라 하겠다. 본 논문에서는 기존의 BLP 모델에서의 사용자 식별과 인증에만 의존한 접근통제를 확장, 강화하는 방안으로, 접근주체를 프로세스의 신뢰성에 기반하여 구분함으로써 비 신뢰적인 프로세스들의 행위를 제한하는 프로세스 기반의 확장된 BLP 모델과 아키텍쳐를 제안했으며, 정보보호의 목적인 기밀성과 무결성이 보장됨을 보였다. 향후 연구로 프로세스 신뢰도의 기준들을 정형화하여 정리하고, 해킹탐지모듈과의 연동을 통해 해킹대응 측면에서의 메커니즘에 관한 연구를 수행하며, 전체적인 참조 모니터의 설계 및 구현을 완성하고자 한다.

5. 감사의 글

본 연구는 한국 정보통신부 정보통신 연구센터 육성, 지원사업의 일환으로 수행되었습니다.

6. 참고문헌

[1] DoD NCSC, "Trusted Computer System Evalution Criteria", Dec. 1985.

[2] Dieter Gollmann, "Computer Security", John Wiley & Sons, 1999.

[3] http://www.redhat.com/support/errata/

[4] Wong, R.M, "A Comparison of Secure UNIX Operating Systems", Computer Security Applications Conference 1990, pp.322-333.

[5] John McLean, "The Specification and Modeling of Computer Security", IEEE Computer, Jan. 1990, pp.9-16.

[7] D.F. Sterne. "On The Buzzword Security Policy", Proc. IEEE Symposium on Security and Privacy, 1991.