SELinux 정책 템플릿 변환기

박호준*, 이재서*, 김정순*, 김민수**, 노봉남*
*전남대학교 정보보호협동과정
**목포대학교 정보보호학과
e-mail:askarone@lsrc.jnu.ac.kr

SELinux Policy Template Converter

Ho-Jun Park*, Jae-Seo Lee*, Jung-Sun Kim*,
Min-Soo Kim**, Bong-Nam Noh*
*Interdisciplinary Program of Information Security, Chonnam National University,
**Division of Information Security, Mokpo National University

요 약

인터넷의 발달에 따라 보안에 위협적인 요소 또한 크게 증가하고 있으며, 이를 극복하기 위한 방법으로 운영체제 수준의 보안 운영체제 연구가 활발히 진행되고 있다. 그 대표적인 연구로는 SELinux 가 있지만 SELinux는 정책의 복잡성으로 인하여 사용자가 이용하기 어렵다는 단점이 존재한다. 본 논문에서는 이와같은 문제점을 해결하기 위해 SELinux 정책 템플릿(SELT)을 이용하여 SELinux의 TE형태로 쉽게 변환하기 위한 SELinux 정책 템플릿 컨버터를 제안한다.

1. 서론

인터넷이 발달하고 보안에 대한 중요성이 강조 되면서 국내외에서 보안 운영체제에 관한 개발 움직임이 활발하게 진행되고 있다. 보안 운영체제의 대표적인 것으로는 미국 국가안전보장국(NSA : National Security Agency) 주도로 개발된 SELinux(Security- Enhanced Linux)이다. SELinux는 유타(Utah)대학에서 개발한 Flask(Flux Advanced Security Kernel) 구조와 TE(Type Enforcement) 정책 모델을 리눅스 시스템에 적용한 것으로 TE 모델을 통해 강제적 접근통제(MAC : Mandantory Access Control) 및 다중등급 보안(MLS : Multi-Level Security) 접근통제 정책을 지원하고 있다[1,2]. 최근 리눅스 커널 2.6에서부터 바닐라(vanilla) 커널에 포함되면서 가장 널리 배포된 보안 운영체제가 되었다.

SELinux는 주체의 대상을 프로세스(process)로하고 객체의 대상으로 파일(file), 디렉터리(directory) 그리고 소켓(socket) 등 리눅스 시스템의 모든 자원(resource)을 목표로 하고 있다. 그리고 권한을 시스템 콜(system call) 수준으로 정의하고 있다. 이처럼 객체의 종류와 개수가 많고 약 764개의 타입과 180,131 개의 규칙으로 이루어져있는 SELinux는 아주 복잡하여 전문지식을 갖고 있지 않은 일반 사용자(보안 정책 관리자)가 이용하기에는 어려움이 많다. 또한 기존 정책간의 복잡한 연관성은 사용자가 쉽게 규칙을 변경, 삭제하기 어렵게 할 뿐만 아니라 새로운 정책을 추가하기 위해서는 기존의 정책들에 대해서 분석해야하는 등 어려움이 있는 상황이다.

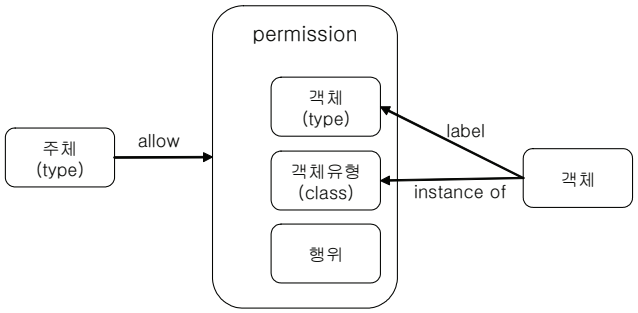
본 논문에서는 SELinux를 보다 쉽게 이용할 수 있도록 하는 SELinux 보안 정책 템플릿을 설명하고 템플릿을 바탕으로 SELinux의 TE형태로 변환을 시켜주는 SELinux 템플릿 변환기를 제시한다.

본 논문의 구성은 2장에서 SELinux의 TE모델에 대해 기술하고, 3장에서는 이를 개선하기 위한 보안정책 설정도구인 SELT대해서 살펴본다. 4장에서 SELT로 표현된 정책을 TE형태로 변환하는 SELinux 보안 정책 템플릿 변환기에 대해 설명하고, 5장에서는 SELinux 정책 템플릿 변환기의 연구 결과 및 분석을 살펴 보고 6장에서는 결론과 향후 연구 과제에 대하여 기술한다..

* 본 연구는 정보통신부 대학 IT 연구센터 육성, 지원사업의 연구결과로 수행되었습니다.

2. SELinux의 TE 모델

SELinux에서 적용하고 있는 TE 모델은 기존 TE 모델보다 발전된 형태의 모델이다. 그림 1은 SELinux TE 모델의 구조를 나타낸 것이다. 주체인 프로세스에게 타입을 할당하고 객체에게 타입을 할당한다. 그리고 할당된 객체 타입과 객체 클래스(class) 그리고 행위로 이루어진 권한(permission)을 주체에게 허용(allow)함으로써 접근통제를 수행하게 된다[3].



(그림 1) SELinux TE 모델 구조

최근의 SELinux는 리눅스 시스템 자원을 커널 객체 클래스 42개와 사용자영역(userland) 객체 클래스 14개로 분류하고 있다. 그리고 각 객체 클래스별로 적게는 1개부터 많게는 31개의 권한의 개수를 갖아 전체적으로 200개가 넘는 권한이 정의되어 있다. 이렇게 많은 객체 클래스와 권한은 일반 사용자에게 어려움을 주는 원인이 되고 있다.

3. SELT 기술언어

SELT 기술언어는 SELinux 의 TE형태의 정책을 보다 쉽게 나타내기위한 SELinux 보안정책 템플릿이다. 그림 2는 기술언어를 간단하게 나타낸 것이다. subject 항목에는 접근 권한을 허용할 프로그램의 주체 타입 이름을 설정한다. 그리고 object 항목에는 주체가 허용할 객체들과 객체의 타입 이름을 추가한다. 그리고 permission 항목에는 주체와 객체 타입의 권한관계를 설정한다[3].

```
subject:
    subject_name    name
    subject_type        type

transition:
    unconfined      { object_type }

object:
    object_type     { path_name | value }

permission:
    object_alias object_type { operations, ... }
```

(그림 2) 보안 정책 템플릿 기술언어

예를 들어 실행 파일인 test 명령어에 대한 보안 정책을 설정하기 위해서는 그림 3과 같이하면 된다. 설정 후 적용한 이후에는 /usr/bin/test를 실행할 경우에 test_t 주체 타입이 test 프로세스에게 부여되고 test 프로세스는 지정된 /tmp/test 파일만을 읽고 쓸 수 있게 된다.

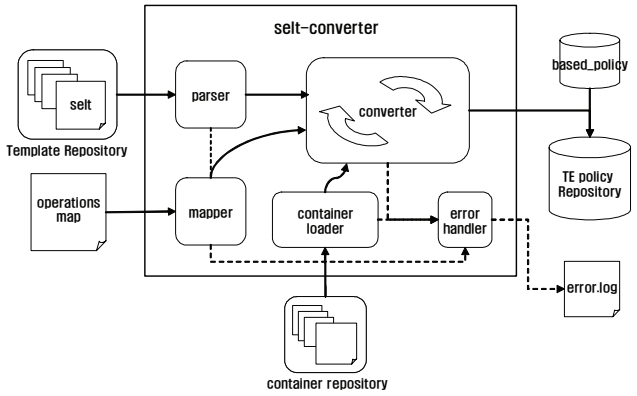
```
subject:
    name            test
    type            binary

transition:
    unconfined      { test_bin }

object:
    test_bin { /usr/bin/test }
    test_file { /tmp/test }

permission:
    test_bin file { execute }
    test_file file { read, write }
```

(그림 3) 보안 정책 템플릿 test 명령어 예제

4. SELT 변환기

4.1 SELT 변환기의 구조

보안 정책 템플릿 변환기는 그림 4와 같이 변환기(converter)와 매퍼(mapper), 파서(parser) 등으로 구성된다. 매퍼는 보안 정책 템플릿의 객체와 권한을 SELinux의 객체 및 권한으로 매핑 시켜 놓은 operations-map을 파싱하여 자료구조화 하고 변환기에 전달하여 주는 기능을 한다. 파서는 기술언어 형태로 정의된 보안 정책 템플릿 파일을 읽어서 자료구조로 만들어 변환기에 전달한다. 변환기는 매퍼와 파서에서 받은 정보와 컨테이너(container) 저장소의 정보 및 기본 정책(based_policy)를 기반으로 하여 SELinux 보안 정책을 생성한다.



(그림 4) 보안 정책 템플릿 변환기 구조

각 모듈에서 발생하는 에러는 에러 처리기가 수집하여 로그로 기록하여 디버깅 정보로 활용할 수 있도록 한다. 표 1은 SELT 템플릿 변환기의 주요 구성요소를 나타낸다.

<표 1> 보안 정책 템플릿 변환기 주요 구성요소

파 일	설 명
based_policy	초기 시스템 상태를 유지하기 위한 최소한의 권한을 포함하고 있는 SELinux 보안 정책
selt	보안 정책 템플릿 파일로 변환될 보안 정책 파일
container	컨테이너의 역할은 규칙 템플릿 변환 과정에서 반복적으로 자주 쓰이거나 그룹화 시킬 필요가 있는 TE 정책을 M4 매크로의 형태로 이용하기 위해서 개발된 것이다.
operations-map	SELinux 권한과 보안 정책 템플릿 권한 매핑 파일

4.2 SELT 컨버터의 구현

SELinux 정책 템플릿 변환기는 크게 6개의 모듈로 구성된다. 각각의 모듈은 템플릿으로 부터 획득한 자료를 바탕으로 SELinux 의 'te' 와 'fc' 파일로 생성하는데 주요 역할을 하는 모듈들이다. 표 2에서 보는 바와 같이 각각의 함수들이 하는 역할들이 정의 되어있다. 해당 함수들에 의해서 SELinux형태로 변환이 가능하다.

<표 2> 보안 정책 템플릿 변환기 주요 모듈

모 듈	설 명
converter_domain_declaration()	도메인 생성 함수로서, 해당 도메인을 정의 하고 타입을 결정지어준다.
converter_role_assignment()	역할 할당 함수로서 템플릿으로 부터 주체타입을 가져와 기본적으로 system_r 에 할당한다.
converter_type_declaration()	타입생성 함수로서 객체 타입과 속성을 가져와 te 형태로 변환한다.
converter_transition_declaration()	도메인 전이 설정 함수로서 템플릿으로 부터 전이 값을 가져와 te파일로 변환한다.
converter_permission_declaration()	권한 생성 함수로서 템플릿에 표현된 권한을 바탕으로 te형태로 변환한다.
converter_filecontext_declaration()	파일 보안 컨텍스트 생성 함수로서 템플릿에 표현된 컨텍스트를 fc형태로 변환한다.

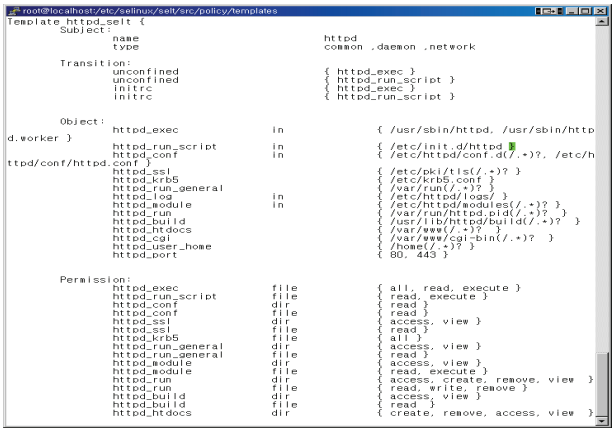
5. 실험결과 및 분석

5.1 분석 환경

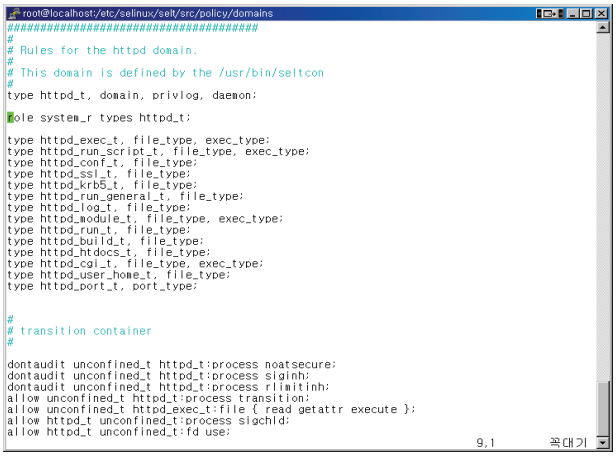
분석환경은 페도라 리눅스 코어 6 배포판을 설치하고 SELinux 보안 정책을 설치하고 적용하였다. 그리고 제안하는 도구인 보안 정책 템플릿 정책과 컨버터를 설치하였다. 실험 항목은 SELinux 기본 보안 정책인 지정 정책(targeted policy)에서 Apache 데몬과 MySql, Samba에 설정한 보안 정책과 보안 정책 템플릿에서 동일한 데몬들에 대한 보안 정책을 설정한 파일 간에 객체 타입과 권한의 개수를 비교 하여 TE정책의 변환 충실도를 분석하였다.

5.2 Apache정책 변환

그림 5는 리눅스 주요 서비스중 하나인 Apache를 SELT정책 템플릿으로 작성한 것이다. 그림과 같이 작성된 정책을 SELT 정책 변환기를 이용하여 SELinux 정책인 'apache.te' 와 'apache.fc' 파일을 생성한다. 그림 6에서는 생성된 'apache.te' 파일 내용을 보여준다. 다음 절에서는 변환기의 완성도를 각각의 정책 별로 비교 분석한다.



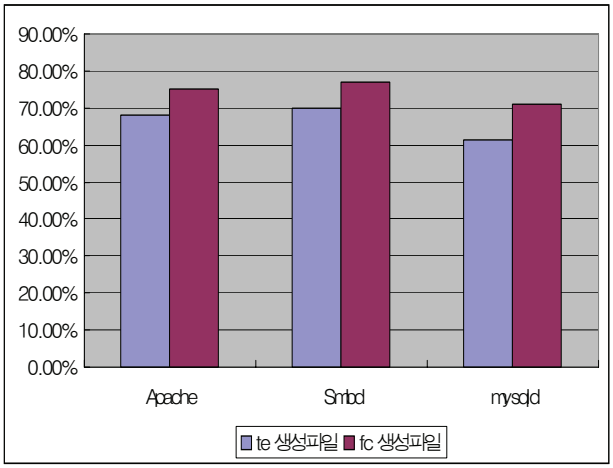
(그림 5) Apache 정책 템플릿



(그림 6) 생성된 Apache.te 파일 내용

5.3 컨버터 TE정책 변환율

그림 7는 SELinux의 기본 정책 배포판에 포함된 표준 정책 데몬 3개와 SELinux 정책 템플릿을 변환기사용을 통하여 얻어낸 각각의 데몬의 정책 정책의 수와 권한의 개수를 비교하여 그 정책의 완성도를 나타낸 그림이다.



(그림 7) 서비스 데몬의 컨버터의 정책 완성도

정책 변환의 결과 'te' 파일에 대해서 약 66.4% , 'fc' 파일의 경우 약 74.4% 정도의 정책 완성도를 보였다. SELinux 에서 제공하는 지정 정책과 SELT 정책 템플릿 변환기를 이용하여 변환한 정책의 결과 70% 정도의 변환율을 보인다.

6. 결론

보안운영체제의 필요성이 대두됨에 따라 SELinux가 개발되었고, SELinux를 보다 쉽고 편하게 사용할 수 있도록 하는 연구들이 진행되어 왔다. SELinux의 복잡한 정책을 쉽게 표현하기 위해 개발된 SELinux 정책 템플릿은 변환기를 통하여 쉽게 SELinux 로 정책 표현이 가능하도록 개발 되었다.

본 논문에서는 SELT템플릿으로 작성된 정책을 'te' 와 'fc' 파일로 생성하여 주는 정책 템플릿 변환기에 대해 제안하였다. 제안된 SELT 정책 변환기를 통해 다음과 같은 이점을 얻을 수 있다.

첫째, SELinux정책생성이 용이하다. SELT 정책 변환기는 SELinux에 대한 지식을 알지 못하더라도 보다 쉽게 표현된 SELT를 이용해 정책설정이 간단하고 SELinux 의 정책 표현이 가능하다.

둘째, SELT 정책 템플릿을 이용함으로써 정책을 통합적으로 관리가 가능하다. SELinux는 'te', 'fc' 와같이 분리되어 있으나 통합된 구조인 SELT정책 템플릿을 이용함으로써 보다 정책 관리가 편리하다.

SELT 정책 변환기를 통해 얻어진 SELinux 의 정책은 70%로서 완벽하게 변환 하지는 않는다. 향후 개선을 통해 정확도를 높이는 과정이 필요하며, SELinux 뿐만 아니라 다른 보안 정책으로 변환할 수 있는 통합적인 변환기 또한 필요하다.

참고문헌

[1] S. Smalley, Configuring the SELinux Policy, NAI Labs Rep. 02-007, 2003. http://www.nsa.gov/selinux/policy2-abs.html

[2] S. Smalley, Configuring the SELinux Policy, Technical report, NSA, Feb. 2002.

[3] 정종민, 김정순, 김민수, 정성인, 노봉남, "SELinux 정책 복잡성 개선을 위한 보안정책 템플릿", 정보보호학회 CISC-S 2006.

[4] Bill McCarty, "SELINUX - NSA's Open Source Security Enhanced Linux", O'REILLY, 2005

[5] David R. Harris The MITRE Corporation "Guided Policy Generation for Application Authors" SELinux Symposium, March 1-3 2006

[6] Tresys Technology, "Security Policy Development Primer for Security Enhanced Linux", 2003

[7] Flask, http://www.cs.utah.edu/flux/flask

[8] SELinux, http://www.nsa.햎/selinux/index.html