SPSL을 이용한 NTFS 다중 사용 권한에 대한 명세 및 검증 [1)]

강미영[0*], 김일곤*, 최진영*, 강인혜**, 강필용***, 이완석***, Dmitry Zegzhda****

*고려대학교 컴퓨터학과
{mykang[0], igkim, choi}@formal.korea.ac.kr,

**서울시립대학교 기계정보공학과
inhye@uos.ac.kr

***한국정보보호진흥원
{kangpy, wsyi}@kisa.or.kr

**** St.-Petersburg State Polytechnical University
dmitry@ssl.stu.neva.ru

The Specification and Verification Using SPSL about NTFS's Multiuser Privileges

Mi-young Kang[0*], Il-Gon Kim*, Jin-Young Choi*
*Dept of Computer Science & Engineering, Korea University

In-Hye Kang**
**Dept of Mechanical and Information Engineering, University of Seoul

Pil-Yong Kang, Wan S. Lee***
***Korea Information Security Agency

Dmitry P. Zegzhda****
**** St.-Petersburg State Polytechnical University

요약

시스템의 안전성을 평가하기위해 프롤로그 기반의 명세 언어인 SPSL을 사용하여 보안 모델을 정형적으로 설계하였다. 보안 모델은 시스템의 3가지 컴포넌트, 시스템 보안 상태(system security states), 접근 통제 규칙(access control rules), 그리고 보안 기준(security criteria)으로 구성된다. 본 논문에서는 NTFS의 다중 사용 권한에 대한 보안 모델을 만들어서 3가지 컴포넌트를 명세하고 안전성 문제 해결 도구인 SPR[1]을 이용하여 검증하였다.

1. 서론

컴퓨터 보안은 가용성의 손실, 비인가 접근, 또는 데이터의 수정에 대한 컴퓨터 자원의 보호를 말한다. 컴퓨터 자원 보호를 위한 모델로는 접근 통제 모델(access control models)과 정보 흐름 모델(information flow models)이 있다. 접근 통제 모델은 HRU 모델[2],SPM 모델[3], TG 모델[4],ESPM 모델[5]등이 있으며 이들 모델은 규칙 변화 상태가 서로 다르게 제안되어 있다. 현재 시스템의 안정성을 평가하기 위해서는 접근 통제 모델이 필요하고 다음 상태의 안정성을 평가하기 위해서는 정보 흐름 모델이 필요하다. SPR(Safety Problem Resolving)은 위의 두 가지 모델을 수용하여 시스템의 상태를 프롤로그[6] 기반의 SPSL(Safety Problem Specification Language)로 상태 보안 모델링하고 접근 통제 규칙(access control rules)을 작성하고 보안 기준(security criteria)에 따라 컴퓨터의 보안성을 평가할 수 있는 정형 검증 도구이다..

본 논문에서는 SPSL를 설명하기 위해 NTFS 다중 사용 권한에 대한 모델을 SPSL로 기술하고 초기 상태에서 거부된 사용 권한은 다른 모든 사용 권한보다 우선한다는 접근 규칙을 명세, 검증하고 발견된 보안상 결함을 수정하는 방법을 설명하고자 한다.

[1)] 본 연구는 한국정보보호진흥원 위탁과제로 수행되었음

2장에서는 SPR에서 입력으로 사용되는 SPSL에 대한 설명을 하고, 3장에서는 NTFS 다중 사용 권한을 SPSL로 명세, 검증하고 보안 위험성을 분석한 후 오류 수정의 방법을 제시한다. 4장에서 결론 및 향후 연구 방향을 제시한다.

2. SPR과 SPSL

SPR(Safety Problem Resolver)은 두 가지 측면에서 안전성 문제를 해결할 수 있다.

첫째, 만일 보안 기준에 대해 주어진 현 시스템 상태를 평가하기를 원한다면, 시스템 보안 상태와 보안 기준, 접근 규칙을 SPR에 입력하면 보안 기준에 따라서 시스템의 안전성 상태를 평가할 수 있다.

둘째, 만약 시스템의 안전성을 평가하기를 원한다면, 초기 상태에서 도달 가능한 시스템 안전 상태들을 생성하고 생성된 상태들의 안전성을 평가한다.

그러므로, SPR은 SPSL로 명세한 초기 시스템 보안 상태(initial system security state), 접근 규칙(access rules), 보안 기준(security criteria)을 입력으로 받아들인다. SPR은 초기 상태의 안전성/비안전성을 검사하고, 현 상태에서 도달 가능한 모든 상태를 생성하고 도달 가능한 상태들의 안전성과 비안정성을 보여 줄 수 있다.

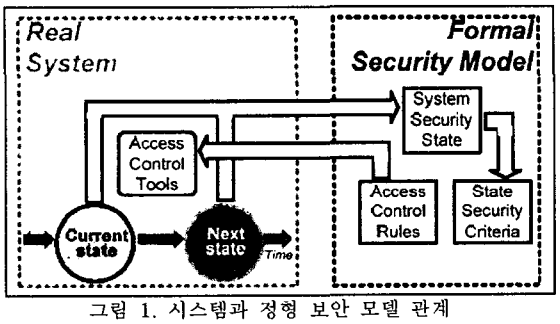

그림 1. 시스템과 정형 보안 모델 관계

[그림1]에서 실세계의 시스템을 정형 보안 모델로 표현하기 위해 시스템 보안 상태(system security State), 접근 통제 규칙(access control rules), 보안 기준(security security criteria)을 프롤로그 기반의 명세 언어인 SPSL로 명세한다. 시스템 보안 상태는 시스템 상태의 추상화이다. 시스템의 요소들은 사용자의 계정, 수행중인 프로그램, 파일, 접근 권한등을 나타내며 주체(subject), 객체(object)로 표현 할 수 있다. 프롤로그 문법으로 데이터베이스의 사실(fact)로 표현한다. 접근 통제 규칙은 시스템 행동의 제한을 표현한다. 시스템의 상태 변화는 시스템 주체(subject)가 접근 통제에 의해 허락된 접근 후에 가능하다. 마지막으로 보안 속성은 안전/비안전 상태를 판별하기 위해 정의한다. 접근 통제 규칙과 보안 속성은 프롤로그의 규칙(rule)으로 명세한다.

3. SPSL을 이용한 NTFS 다중 사용 권한의 명세 및 검증

NTFS 다중 사용 권한 모델은 임의적 보안 모델(discretionary security model)에 근거하여 윈도우 2000

표 1. 접근 권한

Notification	Function
rd	List directory, read data
wd	Create file, write data
ad	Create directory
D	Remove object
ds	Remove subobjects
rp	Read permissions
wp	Change permissions
wo	Change owner

파일 시스템 보안의 핵심 기능을 담당하고 있다. 보안 모델의 요소는 사용자 계정, 사용자 그룹, 파일 시스템의 요소(파일과 폴더)가 있다. 사용자는 정보에 접근하는 활동적인 요소이고, 그룹은 사용자의 단위로 보안 관리자의 관리를 도와준다. 파일 시스템 요소는 정보의 분류에 도움이 된다.

3.1 NTFS 다중 사용 권한

사용자에게 NTFS 허가가 다중으로 부여되었을 때 사용자에게 다중 사용 권한이 유효하다.[7]

- 사용자에게 폴더 사용 권한의 읽기를 부여하고 그 사용자가 속한 그룹에 쓰기 사용권한이 부여된다면 사용자에게 유효한 권한은 읽기/쓰기가 가능하다.
- NTFS 파일 사용 권한은 폴더 사용 권한 보다 우선하다.
- 폴더에 읽기 사용 권한이 부여된 사용자가 폴더에 있는 파일에 변경 가능한 사용 권한이 부여 되면 사용자는 파일 사용에 대한 권한인 변경 권한이 가능하다.
- 거부된 사용 권한은 다른 모든 사용 권한보다 우선한다.

'거부된 사용 권한은 다른 모든 사용 권한 보다 우선한다' 를 모델링하기 위해 [그림2]와 같이 객체 초기 구조에 temp를 만든다. 이 객체들의 사용자는 교수(profs) 그룹과 학생(students) 그룹으로 나눈다. 학생 그룹은 gradesheets 파일에 쓰기 거부 권한(nwd)을 부여한다. 교수 그룹은 gradesheets 파일에 읽기, 쓰기, 권한 (rd,rp,wd)을 부여한다.

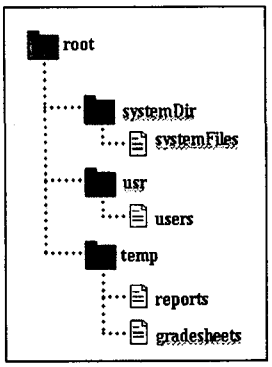

그림 2. 객체의 초기구조

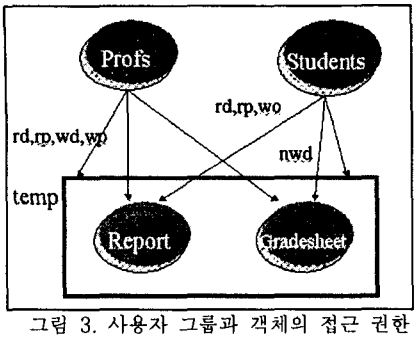

그림 3. 사용자 그룹과 객체의 접근 권한

접근 권한은 [표 1]에 정의되어 있다. 즉, temp 폴더에는 읽기/쓰기 권한이 부여 되고 reports 파일에도 읽기/쓰기가 부여 되지만 gradesheets파일에는 쓰기 거부가 부여한다. 이때 Students 그룹은 report 에는 읽기/쓰기가 가능하기만 gradesheet 파일은 쓰기가 안되고 읽기만 가능하다. SPSL로 [그림 2]의 초기 상태를 기술하면 [그림 4]로 명세한다. 초기 상태는 프로로그의 사실(fact)로 기술한다.

```
subject(pascal,[subjectGroups(profs)]).
subject(kant,[subjectGroups(profs)]).
subject(demian,[subjectGroups(students)]).
subject(kain,[subjectGroups(students)]).

object(temp,[objectType(dir),parentObject(root),objectOwner(admin),
administrators(rd,wd,ad,ds,d,rp,wp,wo),experiencedUsers,
localUsers,profs(wd,wp),students(rd,rp,wd),pascal(rd,rp),
kant,demian,kain,alice,bob,anthony,bill,john,admin]).
object(reports,[objectType(file),parentObject(temp),objectOwner(admin),
administrators(rd,wd,ad,ds,d,rp,wp,wo),experiencedUsers,localUsers,
profs(rd,rp,wd),students(rd,rp,wd),pascal,kant,demian,kain,alice,
bob,anthony,bill,john,admin]).
object(gradesheets,[objectType(file),parentObject(temp),
objectOwner(admin),administrators(rd,wd,ad,ds,d,rp,wp,wo),
experiencedUsers,localUsers,profs(rd,rp,wd),
students(rd,rp,nwd),pascal,kant,demian(nwd,nwp),
kain(nwd,nwp),alice,bob,anthony,bill,john,admin]).
```

그림 4. 초기 상태 명세

프롤로그 문법을 사용하여 NTFS의 특성을 나타내는 규칙은 지면이 짧은 관계로 생략하고, 다중 사용 권한의 중에 '거부된 사용 권한은 다른 모든 사용 권한 보다 우선한다' 의 규칙을 확인하기 위한 보안 범위를 설정한다.

[그림 4]에서 '학생은 gradesheets에 쓰기 권한이 없다' 라고 정의 되어 있다. 보안 범위에서 '학생는 gradesheets에 쓰기 권한이 있다'라고 [그림 4]와 같이 기술한다.

$$\bigcap_{i \in N} \overline{cr_i} = \text{true}$$

보안기준을 cr 이라고 표현했을때, cr_i는 해당 보안시스템에서는 발생하지 않아야 하는 속성을 의미한다. 즉,!testState1(_,_)∧!testState2(_,_)에 대하여 true의 경우 시스템은 안전하다라고 결론을 내린다.

보안 범위를 기준으로 검증하였을 경우 testState1(_,_)의 경우에는 failed의 결과가 str.rep 파일에 출력된다. 발생한 failed의 원인을 찾기 위해 spr.trc파일을 분석하면 Subject(S)가 학생이고 그리고 학생은 Report 객체에 대해서는 쓰기 권한이 존재하므로 failed라는 결론을 내리게 된다. testState2(_,_)와 같이 canWriteFile(S,gandesheets)로 수정하면 succeeded 결과가 출력된다.

```
testState1(S,O):-
        validSubject(S),
        isStudents(S),
        canWriteFile(S,O).

testState2(S,O):-
        validSubject(S),
        isStudents(S),
        canWriteFile(S,gandesheets).
```

그림 5. gradesheets에 대한 보안 기준

4. 결론

시스템의 안정성을 평가하기 위해서, 실세계의 시스템에 대한 보안 모델이 필요하고 또한 보안 모델에 대한 정형적 검증 방법이 요구된다. 본 논문에서는 보안 모델을 프롤로그 기반의 SPSL 명세 언어로 명세하고 보안 검증 도구로 SPR을 사용하였다. 실세계의 시스템을 정형 보안 모델로 표현하기 위한 예로 NTFS 다중 사용 권한의 부분을 SPSL로 모델링하고 검증하였다. 향후 연구로는 windows 2000의 시스템을 SPSL로 명세하고 SPR로 안전성을 검증하며, 나아가 운영체제 시스템, IDS, Firewall등의 시스템의 안정성을 검증하고 분석하는 연구를 하고자 한다.

5. 참고문헌

[1] http://www.ssl.stu.neva.ru/spr/whitepaper.htm
[2] M.A.Harrison, W.L.Ruzzo, J.D.Ullman, Protection in Operating Systems. Communications of the ACM. Vol. 19, Num. 8, August 1976.
[3] R.S.Sandhu, The Schematic Protection Model: Its definition and Analysis for Acyclic Attenuating Schemes, JACM, April 1988.
[4] L.Snyder, Formal Models of Capability-Based Protection Systems', IEEE Transactions on Computers,March 1981.
[5] P.E.Amman, R.S.Sandhu, The Extended Schematic Protection Model, Journal of Computer Security, Vol 1,1992.
[6] J.Wielemaker, SWI-Prolog 5.2 Reference Manual, http://swi-prolog.org, July 2003.
[7] 조성만 외 3, Windows 2000 Server, 혜지원.