보안시스템의 정형화 설계 및 안전성 검증 도구 개발[1)]

김일곤*, 최진영*, 강인혜**, 강필용***, 이완석***, Dmitry P. Zegzhda****

*고려대학교, 컴퓨터학과

**서울시립대학교, 기계정보공학과

***한국정보보호진흥원

****St-Petersburg State Polytechnical University

Formal Modeling for Security System and the Development of Formal Verification Tool for Safety Property

Il-Gon Kim*, Jin-Young Choi*

*Department of Computer Science & Engineering, Korea Univ.

**In-Hye Kang

**Department of Mechanical and Information Engineering, Univ. of Seoul

Pil-Yong Kang, Wan S. Lee***

***Korea Information Security Agency

Dmitry P. Zegzhda****

****St-Petersburg State Polytechnical Univ.

요 약

보안 시스템의 안전성을 분석하기 위해서는, 정형적 방법론을 사용하여 보안 시스템에 대한 이론적인 수학적 모델을 정형적으로 설계하고, 보안 속성을 정확히 기술해야만 한다. 본 논문에서는 보안 시스템의 안전성을 검증하기 위한 보안모델의 구성요소와 안전성 검증방법을 설명한다. 그리고 보안모델을 설계하고 안전성을 분석하기 위한 SEW(Safety Evaluation Workshop)의 전체 구조와 SPR(Safety Problem Resolver) 정형검증도구의 검증방법 및 기능에 대해 소개하고자 한다.

I. 서론

정보통신기술의 발달과 더불어 정보시스템에 대한 의존도와 활용도가 증가되고 있는 반면에, 그에 대한 역기능으로 각종 보안 위협에 쉽게 노출되어 있는 실정이다. 이에 따라 사용자 개인뿐만 아니라 국가 기밀정보를 외부의 악의적인 공격자로부터 보호하기 위해, 보안 운영체제, 침입탐지 시스템, 방화벽등과 같은 보안 시스템을 개발하기 위한 연구가 한창 진행중에 있다. 국내의 경우, 매년 보안시장의 규모가 점차 커져가고 있다. 이런 보안제품을 국외에 수출하기 위해서는 보안평가 체계에 따른 등급심사 과정을 거쳐야만 한다. 국내의 경우 K1부터 K7까지 등급을 분류하고 있으며, K5 이상의 고등급 평가를 받기 위해서는 기

1) 본 연구는 한국정보보호진흥원 위탁과제로 수행되었음.

능, 기본 상계 설계시 정형적 방법론을 이용해야만 한다. 국제공통평가 기준인 CC(Common Criteria)[1]의 경우에도 EAL1부터 EAL7까지 등급을 분류하고 있으며, EAL5 이상의 고등급을 받기 위해서는 정형적 방법론을 사용해야만 한다. 보안 프로토콜의 경우, FDR[2], Murphi[3], NRL Protocol Analyzer[4] 등과 같은 정형검증 도구를 사용하여 보안 프로토콜의 위험성을 분석한 사례는 다수 존재한다. 하지만, 보안 운영체제와 같은 보안 시스템의 안전성을 정형적으로 설계하고 검증하는 도구는 찾아보기는 쉽지 않다.

따라서, 본 논문에서는 보안 시스템의 안전성을 검증하기 위한 보안모델의 구성요소를 설명하고, 보안모델을 설계하고 안전성을 분석하기 위한 SEW(Safety Evaluation Workshop)의 전체 구조와 SPR(Safety Problem Resolver) 정형검증도구의 검증방법 및 기능에 대해 소개하고자 한다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 제 2장에서는 보안모델을 정의한다. 제 3 장에서는 보안시스템의 안전성을 검증하는 방법을 설명한다. 제 4, 5장에서는 보안모델의 안전성을 분석하기 위한 SEW(Security Evaluation Workshop) 구조와 SPR 도구에 대해 간략히 소개하고, 제 6장에서는 간단한 MAC 기반 접근통제 모델을 SPSL로 명세하고 안전성을 분석한 예제를 설명하고 마지막으로 결론 및 향후 연구방향을 제시하고자 한다.

II. 본문

1. 보안모델

보안이란 용어는 매우 광범위하게 사용되어 오고 있다. 보안이란 일반적으로 비밀성, 무결성, 가용성의 3대 요소를 내포하는 용어로 사용되어 오고 있다[5]. '비밀성'이란, 사용자의 비밀정보가 비인가자에게 노출되지 않아야하는 속성을 의미한다. '무결성'이란, 사용자의 승인 없이, 정보에 대한 변조가 이루어지지 않아야 한다는 속성을 나타낸다. 그리고 '가용성'이란 사용자가 언젠가는 해당 서비스를 이용할 수 있어야 한다는 속성을 나타낸다. 예를 들어, 서버에 접속해서 정보를 이용하려 시도하는 클라이언트라면, 언젠가는 서버에 접속해서 해당 서비스를 이용할 수 있어야 한다. 보안모델을 정의하는 문헌은 몇 가지가 있지만, 일반적으로 "보안모델이란, 보안 시스템의 비밀성 요구사항에 대한 정형적 표현이다"라고 정의되어진다[6]. 자세히 설명하면, 보안모델이란 대개 접근통제모델이 반드시 갖추어야하는 요구사항에 대한 정형적 명세 모델을 의미한다. 접근통제는 접근통제규칙을 기반으로 객체(object)에 대한 주체(subject)의 접근을 통제하게 된다. 접근통제모델은 보안정책에 따라 크게 세 가지로 분류할 수 있다.

1) DAC(Discretionary Access Control) :
임의적 접근통제는 주체의 접근권한에 따라 객체에 대한 접근을 통제하는 방법이다.

2) MAC(Mandatory Access Control) :
강제적 접근통제는 주체의 보안레이블과 주체가 접근하고자 하는 객체의 보안레이블을 비교하여 보안 정책에 합당한 접근통제 규칙에 의해 접근통제 하는 방법이다.

3) RBAC(Role-Based Access Control) :
RBAC 모델은 사용자가 특정한 역할을 맡아서 그 역할에 맡는 권한만을 갖도록 설정하고 있다. 이 권한을 통해 주체에 대한 객체의 접근을 통제하는 방법이다.

본 논문에서는 보안시스템을 정형적으로 설계하고 안전성을 분석하기위해, 앞에서 언급한 사항과 달리 '보안모델'을 새롭게 정의하고 있다. 앞으로 사용할 '보안모델'이라는 용어는 세 가지의 컴포넌트로 이루어져 있다. 첫 번째 컴포넌트는 보안시스템의 상태를 나타내기 위한, '시스템 보안 상태(System Security State)'이다. '상태'란 보안시스템에 존재하는 사용자 계정, 파일, 사용자 권한 등을 가리킨다. 두 번째 컴포넌트는 '접근통제규칙(Access Control Rules)'이다. 세 번째 컴포넌트는 '보안 기준(Security Criteria)' 이다. '보안 기준' 이란 보안 시스템이 만족해야 하는 속성을 나타낸다.

2. 보안시스템의 안전성 검증 방법

보안시스템의 안전성을 검증하기 위해, 본 논문에서는 유한상태기계로 보안시스템의 행위를 나타내었다. 유한상태기계에서 상태 정보는 '시스템 보안 상태'를 통해 추출한 사용자 계정, 파일, 접근권한 등을 포함하고 있다. 그 다음은 '접근통제규칙'에서 규칙을 통해 상태간의 전이를 표현하게 된다. 마지막, 보안시스템의 행위를 표현한 유한상태기계가 '안전성'을 위배하는 상태에 도달하는지를 체크하게 된다. '안전성'이란 보안 속성중에서 비밀성이 위배되는 상황을 의미한다. 정확히 말하면, 비접근 권한을 갖고 있는 사용자에게 중요한 정보가 노출되는 경우를 가리킨다. 본 논문에서 설명하고 있는 보안시스템의 안전성 검증 방법에서는 다음과 같은 두 가지 경우에 보안시스템이 안전하다고 판단한다. 첫 번째는 보안시스템의 행

위를 나타내는 유한상태기계의 초기상태가 안전성을 만족하고 있을때, 두 번째는 시스템의 상태 정보가 변경되는 경우에, 도달가능한 모든 상태들 간의 전이를 통해 안전성을 위배하는 상태를 찾아내지 못한 경우에 보안시스템이 안전하다고 결정한다. 상태들 간의 전이를 통해 보안시스템의 안전성을 결정하는 방법은 그림 1과 같이 나타낼 수 있다.

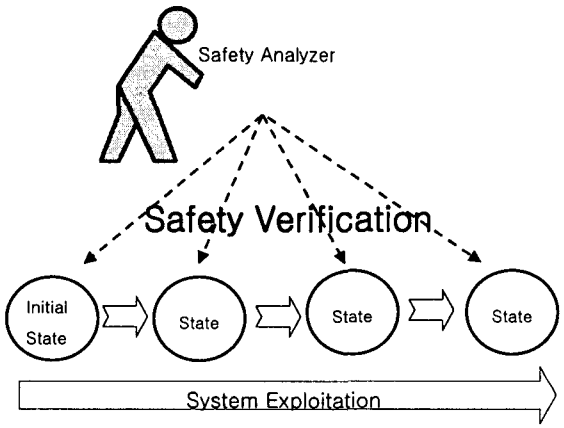

그림 1: 보안 시스템의 안전성 검증방법.

3. SEW

이 논문에서 언급하고 있는 보안시스템이란 운영체제 시스템, 침입탐지시스템, 방화벽등을 그 대상으로 하고 있다. 보안시스템의 안전성을 분석하기 위해서, 'SEW(Safety Evaluation Workshop)'라고 불리는 보안 시스템 설계 및 분석 구조체계를 사용하고자 한다. SEW을 구성하고 있는 중요 컴포넌트들은 그림 2에 잘 나타나 있다.
SEW를 구성하고 있는 각각의 중요 컴포넌트들의 기능을 살펴보면 다음과 같다.

1). System State Analyzer :
보안모델의 상태를 자동추출

2). Security Criteria Manager :
보안모델이 만족해야 하는 해당 보안속성을 GUI 형태로 입력

3). Scopes :
가. State Security Criteria Scope :
보안속성(예, No Read Up, No Write Down등)
나. Access Control Rules Scope :
접근통제규칙(예, Security Reference Monitor)
다. Model-related System Security Scope :
보안모델 상태(예, 주체(subject), 객체(object), ACL등)

4). SPR : 프롤로그(Prolog)언어 기반의 정형검증 도구, SWI-Prolog[7]로 구현

5). SPSL(Safety Problem Specification Language) :
3번에서 언급한 3개의 Scopes를 나타내기 위한 프롤로그 기반의 명세언어

6). Security Flows Explorer :
SPR 도구를 통한 보안취약점 추적(프롤로그 기반의 역추적 결과들)

7). Evaluation Reporter :
보안취약점에 대한 최종 보고서

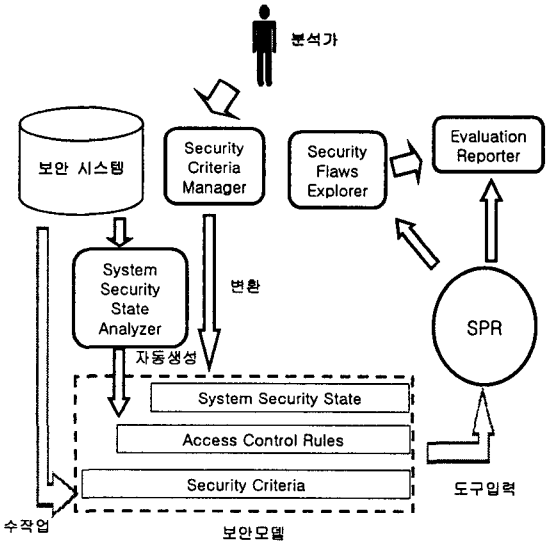

그림 2: SEW 구조.

3. SPR

SPR(Safety Problem Resolver)은 보안시스템의 안전성을 분석하기 위한 정형검증도구로서, 프롤로그 언어를 기반으로 하고 있으며, 3개의 Scopes를 입력파일로 받아들인다. SPR 도구의 API는 C++언어로 작성되어 있다. 3개의 Scopes 입력파일들은 보안 모델을 나타내게 된다. 즉, SPR 도구

에서 입력으로 받아들이는 보안모델은 앞에서 언급하였듯이, 3개의 컴포넌트로 구성되어 있다.

보안모델 = 시스템 보안상태 + 접근통제규칙 + 보안기준

4. 예제

앞에서 언급하였듯이, SPR 도구를 이용하여 보안시스템의 안전성을 분석하기 위해서는 3개의 Scopes로 구성되어 있는 보안모델을 입력파일로 받아들여야 한다. 제4장에서는 간단한 접근통제모델을 어떻게 SPSL로 명세하고 SPR 도구를 통해 해당 보안속성을 검증하는지 살펴보도록 하겠다. 표 1은 3개의 주체와 3개의 객체로 구성된 간단한 MAC 기반 접근통제모델의 접근통제 리스트를 보여주고 있다.

표 1: 접근통제 리스트

객체 / 주체	Object1	Object2	Object3
High Group	읽기 쓰기	읽기 쓰기	읽기
Low Group			읽기
Subject1	읽기 쓰기	읽기 쓰기	읽기 쓰기
Subejct2	읽기 쓰기	읽기 쓰기	읽기
Subject3			읽기 쓰기

위의 표에서 보여주고 있는 MAC 기반 접근통제모델은 상위(High)와 하위(Low) 그룹으로 나뉘어져 있으며, 상위그룹에는 Subject1, Subject2, Object1, Object2가 속해있고, 하위그룹에는 Subject3와 Object3가 속해있다. 위 예제에서 Subject는 사용자를 나타내며, Object는 사용자가 소유하고 있는 파일들을 가리키고 있다. 그리고 상위 모델의 경우 다음과 같은 보안속성을 보장해야만 한다.

1) No Read Up:
   하위그룹은 상위그룹의 객체를 읽을 수 없다.
2) No Write Down:
   상위그룹은 하위그룹의 객체에 쓸 수 없다.

제 4장에서 언급하였듯이, 보안모델의 안전성을 평가하고 분석하기 위해서는 3가지의 입력파일을 SPSL로 명세한 후, SPR 도구를 통해 그 취약점을 확인하게 된다. 3개의 입력파일은 각각 다음과 같은 .sc라는 파일 확장자명을 가져야 한다. 위의 예제에 대한 시스템 보안상태는 그림 3과 같이 표현 될 수 있다. 그림 3은 앞에서 언급한 MAC 기반 접근통제모델의 시스템 보안상태를 SPSL로 기술한 부분을 나타내고 있다. 이 접근통제모델이 No Read Up, No Write Down의 보안속성을 만족시키는지 체킹하기 위해, 그림 4와 같이 보안기준을 표현하였다. 보안기준은 모델체킹에서 사용되는 속성(property)과 같은 의미로 사용되고 있다. 보안기준을 cr 이라고 표현했을때, cr_i는 보안시스템에서는 발생하지 않아야 하는 속성을 의미한다. SPR도구에서 보안기준은 다음과 같은 형식으로 표현하고 있다.

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

```
subjectAttr(subjectGroups).
subject(s1,[subjectGroups(high)]).
subject(s2,[subjectGroups(high)]).
subject(s3,[subjectGroups(low)]).
objectAttr(objectType).
objectAttr(high).
objectAttr(low).
objectAttr(s1).
objectAttr(s2).
objectAttr(s3).
object(o1, [objectType(file),
high(rd,rp,wd,wp), low, s1(rd,rp,wd,wp),
s2(rp,rd,wd,wp), s3]).
object(o2, [objectType(file), high(rd,rp,wd,wp),
low, s1(rd,rp,wd,wp), s2(rd,rp,wd,wp), s3]).
object(o3, [objectType(file), high(rd,rp),
 low(rd,rp), s1(rd,rp,wd,wp), s2(rd,rp),
s3(rd,rp,wd,wp)]).
```

그림 3 : SPSL을 이용한 시스템 보안상태 명세.

모든 시스템의 상태에서 위와 같이 보안상 문제점을 발생시키는 보안 기준이 발생하지 않았을 경우, 우리는 보안 시스템이 안전하다고 말할 수 있

다. 따라서, testState1(S,O)과 testState2(S,O)에 대한 보안기준이 발생하는지 체킹하게 되면, SPR 도구는 그림 5와 같은 'spr.rep' 결과 파일을 생성하게 된다.

```
testState1(S,O):-
        validSubject(S),
        isFile(O),
        canReadFile(S,O),
        not(isGroupMember(S,high)),
        O=o1,
        O=o2.

testState2(S,O):-
        validSubject(S),
        isFile(O),
        canWriteFile(S,o3),
        not(isGroupMember(S,low)).
```

그림 4 : SPSL을 이용한 보안기준 명세.

```
/*
*    SPR report file
* File contains criterion and its results about
its safety
*/

testState1(_,_)          succeeded
testState2(_,_)          failed
```

그림 5: spr.rep 파일 출력결과.

testState2에 대한 보안기준에 대해 'failed'가 발생했다는 사실은 No Write Down에 대한 보안속성을 위배했다는 것을 의미한다. SPR 도구에서 생성한 프롤로그 기반의 역추적 결과물을 자세히 살펴보면, 표 1과 그림 3에 나타나 있듯이, subject1이 object3에 대해 읽기, 쓰기 권한이 모두 설정되어 있기 때문에 위와 같은 결과가 생성되었음을 알 수 있다. 본 논문의 지면 사정상 접근통제규칙에 대한 SPSL 코드는 생략하였다.

Ⅲ. 결론

보안제품을 생산하기 위해서는 보안 개발자들이 보다 손쉽게 보안모델을 추출, 명세하고 해당 요구사항을 검증할 수 있는 정형검증도구의 개발이 절실히 필요한 실정이다. 본 논문에서는 정형적으로 보안모델을 설계하고 안전성을 검증하기 위해 개발한 SPR 도구에 대해 설명하였다. 정형적 설계 및 분석 방법을 통한 고등급 보안시스템의 개발은 결국 시스템의 안전성 및 보안성을 보장하게 되고, 국내 뿐만 아니라 국외 보안시장에서 국가 경쟁력을 키워나가는데 매우중요한 역할을 차지하게 될 것이다. 물론, SPR 도구의 활용성을 높이기 위해서는 IDS, Firewall, 운영체제 시스템과 같은 보다 실질적이고, 다양한 보안 시스템을 SPSL로 명세하고 검증한 사례에 대한 활용가이드가 필요하다. 향후 연구방향으로는 SEW의 각 주변도구를 개발하여 보안모델을 명세하고 분석하기위한 사용자의 편이성을 높이고자 한다.

참고문헌

[1] Common Criteria for Information Technology Security Evaluation Version 2.1, August 1999.

[2] Formal Systems(Europe) Ltd. Failure Divergence Refinement-FDR2 User Manual, Aug. 1999.

[3] C. Mitchell, "Automated Analysis of Cryptographic Protocols Using Murphi", IEEE Symposium on Security and Privacy, 1997.

[4] C. Meadows, "The NRL Protocol Analyzer: An Overview", Journal of Logic Programming, 1994.

[5] R. Shirey. RFC 2828, Internet Security Glossary, Network Working Group, May 2000.

[6] J. Mclean, "Security Model", In Encyclopedia of Software Engineering, Wiley Press, 1994.

[7] J. Wielemaker, SWI-Prolog 5.2 Reference Manual, http://swi-prolog.org, July 2003.