SPIN을 이용한 침입탐지 메커니즘의 정형적 설계방법[1)]

방기석[O*] 김일곤[*] 강인혜[**] 강필용[***] 이완석[***] 최진영[*]
[*]고려대학교 컴퓨터학과
{kbang[O], igkim, choi}@formal.korea.ac.kr

[**]서울시립대학교 기계정보공학과
inhye@uos.ac.kr

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

Formal Design of Intrusion Detection Mechanism using SPIN

Ki-Seok Bang[O] Il-Gon Kim Jin-Young Choi
Dept. of Computer Science and Engineering, Korea University
In-Hye Kang
Dept. of Mechanical and Information Engineering, University of Seoul
Pil-Yong Kang, Wan S. Yi
Korea Information Security Agency

요 약

고등급의 침입 탐지 시스템 평가를 받기 위해서는 반드시 정형적인 방법론을 적용하여 시스템을 설계하고 검증해야 한다. 그러나 침입 탐지 시스템의 설계에 적합한 정형기법을 선정하기는 매우 어렵다. 본 논문에서는 정형 기법의 일종인 모델 체킹 방법론을 침입 탐지 메커니즘의 설계에 적용하는 방법을 제안하고, 고등급 침입 탐지 시스템의 개발에 사용할 수 있는 방향을 제시한다.

1. 서 론

컴퓨터 시스템이 발달하고 전 세계의 시스템이 인터넷을 통해 연결되면서 많은 정보가 빠른 속도로 교환되고 있다. 특히, 컴퓨터 통신 시스템의 발전은 많은 다른 분야의 발전을 유도하고, 새로운 기술의 개발 속도를 매우 빠르게 하고 있다. 이렇듯 최근 컴퓨터 통신 시스템에 대한 의존도는 급격하게 증가하고 있다. 그러나 컴퓨터 통신 시스템의 발전이 가져오는 역기능으로 알지도 못하는 사이에 각종 위협에 자신의 시스템이 노출되어 있는 것이 현실이다. 개인뿐만 아니라 대부분의 컴퓨터 시스템은 시스템의 정보를 유출시키고 시스템의 동작을 무력화 시키고자 하는 많은 보안 위협에 노출되어 끊임없이 공격당하고 있는 것이 사실이다. 이에 따라, 외부로부터의 위협으로부터 자신의 시스템을 보호하고자 하는 연구 및 노력이 매우 활발하게 이뤄지고 있다. 국내/외적으로 정보 보호 시스템 혹은 보안 제품의 개발을 촉진시키고 있으며 보다 안전한 시스템을 개발하고자 많은 투자를 아끼지 않고 있다. 또한, 개발된 보안 제품 및 시스템의 안전성 및 보안성을 보장하기 위해 제품을 평가하는 제도를 채택하고 있다.[1] 국내에서는 침입 탐지 시스템의 평가를 위해 정보보호 진흥원에 의해 K등급[1]을 제정하고 고품질 정보보호 제품의 평가를 추진하고 있다. K등급에 따르면 K1부터 K7까지의 7단계의 등급을 부여하고 있으며 그 중 K5 이상의 등급에서는 설계시부터 정형적인 방법론을 따르도록 하고 있다. 해외에서도 여러 나라에 의해 정보 보호 제품의 평가 및 등급을 부여 하고 있다. 최근에는 국제 공통 평가기준인 CC(Common Criteria)[2]를 제정하여 서로 다른 나라에서 개발한 보안 제품에 대해서도 공통된 기준으로 평가를 수행하고 있다. 이 평가 기준에서도 EAL5이상의 고등급을 부여받기 위해서는 반드시 정형적인 설계 방법을 이용해야 한다. 그러나 정보 보호 제품에 사용되는 각종 보안 모델 및 정보 보호 메커니즘을 정형적으로 설계하기는 매우 어렵다. 특히, 침입자의 행위를 모델링하고, 그 행위에 따른 보안 제품의 반응을 모델링하기 위해서는 따라서, 현재까지 고등급의 평가를 받은 고품질 정보 보호 제품이 그렇게 많지는 않다.

본 논문에서는 정형 검증 도구인 SPIN[3]을 이용하여 이러한 정형적 설계의 어려움을 극복할 수 있는 방법을 제시하고자 한다. 정형 설계 및 검증 기법을 함께 가지고 있는 모델 체커인 SPIN을 활용하면 침입자의 공격에 대한 보안 메커니즘의 동작 여부를 시뮬레이션을 통해 쉽게 확인할 수 있고, 구현 후의 시스템과의 일치성을 확인할 수 있는 장점이 있다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 상태 기계 기반의 정보 보호 메커니즘의 설계에 대해 설명하고, 3장에서는 모델 체커인 SPIN을 이용한 침입 탐지 메커니즘의 설계 및 시뮬레이션에 대해 논한다. 그리고 4장에서 논문의 결론을 맺고자 한다.

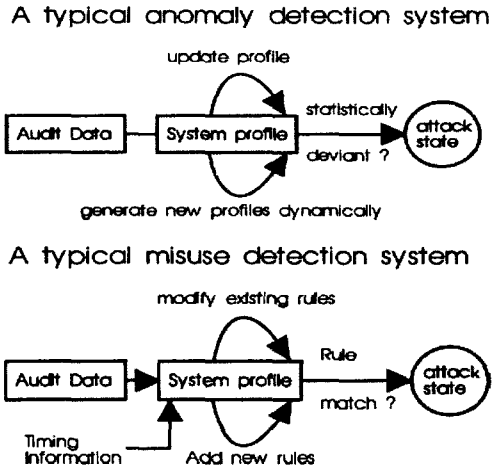
1) 본 연구는 한국정보보호진흥원 위탁과제로 수행되었음.

2. 상태 기계 기반의 침입 탐지 메커니즘 설계

2.1 침입 탐지 메커니즘

시스템의 내부에서 동작하는 각종 자원 및 자료를 비인가 된 접근으로부터 보호할 수 있는 메커니즘을 설계하는 것은 매우 중요하다. 그러나 완벽하게 모든 위협을 방어하는 것은 현실적으로 불가능하다. 대신 후에 발생할 수 있는 위협적인 접근을 탐지하여 사전에 방지하는 연구가 활발히 진행되고 있다.[4] 이러한 방법을 침입탐지라고 한다. 이미 1980년대부터 침입탐지에 대한 정의를 내리고 그 종류를 분류하고 있다. 기본적으로 침입이라 함은 시스템의 정보에 접근하고, 정보를 조작하거나 시스템을 불안정하도록 만들 수 있는 비인가 된 접근이라고 정의한다.[4][5]

이러한 침입의 정의에 따라 매우 많은 종류의 침입이 시도되고 있으며 그러한 다양한 침입 시도에 따라 여러 종류의 침입 탐지 메커니즘이 연구되고 개발되고 있다. 대표적으로 변칙 탐지 시스템(Anomaly Detection System)[4][5][6]과 오용 탐지 시스템(Misuse Detection System)[4][5][6]으로 분류할 수 있다. 변칙 탐지 시스템은 정상적인 행동으로 간주하는 모든 시스템의 동작을 저장해 놓고 그 외의 동작을 야기하게 되면 침입이라고 판단하는 방법이다. 이에 비해 오용 탐지 시스템은 알려진 공격의 패턴을 저장해 놓은 뒤 저장된 공격 패턴과 동일한 행위를 하는 이벤트 혹은 명령의 순열이 발생할 경우 침입으로 판단하는 시스템이다.



[그림 1] 침입 탐지 시스템의 동작 원리

본 연구에서는 오용 탐지 시스템을 대상으로 정형 명세를 적용하였다.

2.2 상태 기반 분석 방법

오용 탐지 시스템의 한 방법으로 모델 기반 탐지 방법[5][6]이 있다. 이는 특정한 행위의 시나리오를 설정하고 이를 침입 시나리오로 분류해 놓는다. 그 후 시스템에 들어오는 이벤트 혹은 명령어들의 순서를 수집하여 자신이 알고 있는 공격의 시나리오와 동일한지를 비교하고 동일한 경우 침입으로 판단하게 된다. 이러한 탐지 방법은 입력되는 행위를 기준으로 탐지 시스템의 상태를 전이시켜 최종 상태가 침입상태로 전이되는가를 확인하는 상태기계의 전이를 기반으로 분석을 하게 된다. 이러한 상태 기반 분석 방법에 따르면 탐지 시스템 자체가 상태 전이도로 모델링 되고, 각 상태에서 특정한 이벤트들에 의한 불리언 값을 세팅해 나가면서 전이를 한다. 모든 전이가 끝난 후의 상태를 확인하여 침입상태인지를 분석해 내는 방법이다.[4][6][7]

2.3 모델 체킹과 SPIN

모델체킹[3]은 유한 상태 시스템의 정확성을 자동으로 정형 검증하는 기술이다. 즉, 시스템이 동작하는데 있어서 지켜야 할 사항과 발생해서는 안 되는 상태에 대한 논리적인 증명을 통해, 시스템의 정확성을 확인하는 과정이다. 모델체킹은 많은 장점과 단점을 동시에 갖고 있지만, 하드웨어의 회로나 통신 프로토콜과 같은 매우 복잡한 시스템을 성공적으로 정형 검증 할 수 있다. 모델체킹은 유한 상태 시스템을 검증하기 때문에 검증 과정이 자동화되어 있다. 따라서 검증을 수행함에 있어 사람의 개입이 매우 적기 때문에 보다 정확하며 검증 과정이 편리하다. 또한 검증 과정이 일반적으로 시스템이 가질 수 있는 모든 상태 공간에 대해 전역 탐색을 사용하기 때문에 주어진 자원이 충분하다면 매우 큰 시스템에 대해서도 그 시스템의 동작에 대해 yes 혹은 no를 항상 결정할 수 있다.

SPIN은 통신 프로토콜의 설계 및 검증을 위해 개발된 소프트웨어 모델 체커이다. 통신 소프트웨어를 설계하기 위해 개발되었기 때문에 기본적으로 프로세스 단위로 동작을 명세한다. 각 프로세스 간의 통신을 위해 전역 변수 및 통신 채널을 설정할 수 있고, 동기/비동기 통신을 모두 구현할 수 있다. 프로세스들은 동시 수행을 원칙으로 하며 비결정적인 선택 및 반복 구문을 지원하여 공격자 모델을 명세할 때 임의적인 공격 패턴을 만들어 낼 때 용이하다.

3. SPIN을 이용한 보안 메커니즘의 설계

3.1 SPIN을 이용한 모델링

침입 탐지 모델의 규칙은 다음과 같다. 공격자는 자신이 알고 있는 공격 패턴 중 하나를 선택하여 그 공격 패턴을 이용해 침입을 시도한다. 이 때 공격 패턴은 이벤트의 발생을 이용해 모델링 한다. 이벤트들은 임의적으로 선택이 되기 때문에 매우 많은 순열이 발생 가능하다. 그 순열 중 실제 공격으로 인정되는 경우는 단 한 가지로 제한한다. 침입 탐지 메커니즘 역시 자신이 알고 있는 공격 패턴을 저장하고 있다. 이것을 공격 규칙으로 설정하고 있다. 외부로부터 들어오는 이벤트들을 모니터하고 있다가 특정 이벤트가 들어오면 침입 가능성이 있다고 판단하게 된다. 이러한 판단이 이뤄진 후 들어오는 이벤트들을 검사하여 공격 패턴과 동일한 순열을 이룰 때 침입이 이뤄진다고 판단하게 된다. 이벤트가 입력되는 순서가 공격의 순서와 맞지 않다면 정상적인 동작으로 판단하게 될 것이다.

```
inline attack1 (a1, b1, c1, d1) {
  do
  :: check?rev -> break;
  :: d_step{att!a1; printf("MSC: attack = %d₩n", a1);}
  :: d_step{att!b1; printf("MSC: attack = %d₩n", b1);}
  :: d_step{att!c1; printf("MSC: attack = %d₩n", c1);}
  :: d_step{att!d1; printf("MSC: attack = %d₩n", d1);}
  od
}
active proctype receiver() {
  byte  income;
  do
  :: att?income ->
    if
    :: atomic {  if
                 :: income == 1 -> check1 = 1;
                 :: skip;
                 fi; }
                              ...
    :: atomic{ if
               :: (income == 4) && (check3 == 3) ->
                  check4 = 4;
                  rev = 1; check!rev; break;
               :: skip;
               fi;}
     fi;
   od; }
```

[그림 2] SPIN을 이용한 침입탐지 메커니즘 명세

3.3 시뮬레이션 및 동작 확인

[그림 2]와 같이 명세된 침입 탐지 메커니즘은 SPIN에서 제공되는 시뮬레이션을 통해 그 동작을 쉽게 확인할 수 있다. SPIN은 변수의 설정 및 변화에 대한 모든 리스트를 출력해 주고 통신을 하는 프로세스 간의 교환을 MSC(Message Sequence Chart)의 형태로 출력해 주기 때문에 쉽게 그 동작을 확인할 수 있다.

시뮬레이션 결과를 보면 공격자에 의해 특정한 공격 패턴이 발생되고 그것을 침입 탐지 시스템에서 갖고 있는 공격 패턴과 비교하게 된다. 즉, 패턴 매칭에 의해 침입 가능성 여부를 판단하게 된다. 비교 결과 공격의 패턴에 부합되는 입력이 발생하게 되면 즉시 공격이 발생했음을 출력하게 된다.

```
MSC: attack = 1
MSC: attack = 2
MSC: attack = 3
MSC: attack = 4
    In coming attacks are 1 2 3 4,
Attack is revealed!!!
```

[그림 3] 침입탐지 동작 시뮬레이션 결과

[그림 3]에서 보는 바와 같이 공격 순열을 판단하여 순서에 맞는 공격이 발생했을 경우 공격으로 판단하게 된다. 그러나 이러한 패턴 매칭에 의한 침입 탐지 시스템은 공격 패턴의 작은 변화를 찾아내지 못한다는 단점이 존재한다. 즉, 동일한 공격을 반복해서 보내거나 공격 패턴을 조금만 변경하면 탐지가 불가능하다. 이는 모델 기반 침입 탐지 시스템이 갖는 가장 큰 단점이다. 본 모델에서도 공격자의 공격 패턴이 다양함에도 불구하고 탐지 시스템이 알고 있는 공격 패턴만을 찾아냄을 알 수 있다. 이 문제점은 모델 기반의 침입탐지 시스템이 갖고 있는 고유한 문제점이다.

4. 결론 및 향후 연구

본 연구에서는 모델 기반의 침입탐지 시스템을 모델 체커인 SPIN을 이용해서 명세하고 그 동작을 확인하였다. 컴퓨터 시스템과 정보 통시 시스템의 발전에 따라 개인 정보 보호 및 시스템의 침입을 막기 위한 연구 및 개발이 활발해 지고 있다. 침입 탐지 시스템을 비롯한 각종 정보 보호 제품 및 보안 시스템은 고품질의 시스템을 개발하기 위해 각 제품에 맞게 평가받고 있다. 각 평가 기준에서는 단계별 평가 기준을 정해놓고 있으며 고등급의 평가를 위해서는 반드시 정형적인 방법론을 사용해서 개발해야만 한다. 그러나 보안 시스템의 경우에는 정형적 방법론의 적용 자체가 매우 어려우며 고등급의 평가가 어려운 것이 현실이다.

본 연구에서는 이런 문제점을 해결할 수 있는 방법으로 모델체킹 도구인 SPIN을 이용해서 침입 탐지 시스템을 명세하고 그 동작을 확인하였다. 모델 체커인 SPIN은 그 사용이 간편하고 명세 방법도 매우 쉬운 편이다. 그리고 명세된 시스템의 시뮬레이션 및 특성을 확인하기도 매우 편리하다.

SPIN을 이용하여 침입탐지 시스템을 모델링하고 그 동작을 확인함으로써 설계하고자 하는 침입탐지 시스템의 동작상 정확성을 확인할 수 있다. 그리고 구현된 침입 탐지 시스템과의 비교를 통해 구현의 정확성을 확인하여 올바르게 시스템이 구현되었는지를 확인할 수 있는 기능도 제공할 수 있게 된다.

현재 대상으로 하고 있는 침입 탐지 시스템은 모델 기반 침입 탐지 시스템이다. 따라서 공격 패턴이 이미 알려져 있고 탐지 시스템 내부에 설정되어 있는 공격에 대해서만 탐지해 낼 수 있다. 정형적 방법론 중 상대적으로 쉽고 빠른 모델체킹을 보안 시스템의 정형적 설계에 적용한다면 설계자 및 평가자들에게 공통된 개발 기준을 제공할 수 있으며 고등급 평가에 적용할 수 있을 것이다. 향후에는 매우 다양한 침입 탐지 시스템 및 보안 시스템의 모델링에 모델체킹 방법론을 적용해 볼 수 있을 것이다.

참고문헌

[1] 정보보호시스템 평가인증 가이드, 한국정보보호진흥원, 2002.

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

[3] E. M. Clarke, O. Grumberg, and D. A. Peled, "Model Checking", MIT Press, 1999.

[4] M. Bishop, "COMPUTER SECURITY", Addison Wesley, 2003.

[5] D. E. Denning, An Intrusion Model, IEEE TSE, vol. SE-13, no. 2, pp. 222-232, 1987.

[6] A. Sundaram. An Introduction to Intrusion Detection, ACM Crossroad, 1996.

[7] K. Ilgun, R. A. Kemmer, P. A. Porsas, State Transion Analysis: A Rule-Based Intrusion Detection Approach, IEEE TSE, 1995.