자동화된 침입대응 시스템 설계에 관한 연구

이보경°, 이호재, 김영태, 최중섭
한국정보보호진흥원
{bklee°, leehj, ytkim, jschoi}@kisa.or.kr,

A Study on the Design Automated Intrusion Response System

Bokyoung Lee°, Hojae Lee, Youngtae Lee, Joongsup Choi
Korea Information Security Agency

요 약

침입이란 컴퓨터 자원의 무결성, 비밀성 및 가용성을 저해하고, 시스템의 보안정책을 파괴하는 행위로서, 지금까지 연구되어 온 호스트 기반, 다중 호스트 기반 및 네트워크 기반 침입탐지 시스템만으로는 침입이 발생한 사후에 판단, 추적이 어려우며, 침입 중 차단이 불가능하므로 대규모 분산 시스템에 대한 침입에 종합적으로 대응하기 어렵다. 따라서 본 글에서는 지능화된 공격에 자동대응이 가능하도록 하기 위해 공격의 심각도 및 피해정도 그리고 침입탐지시스템이 탐지능력의 신뢰도에 따라 대응 수준 및 대응방법이 결정되도록 하는 자동화된 침입대응 시스템 및 사용된 메커니즘에 대해 설명하고자 한다.

1. 서 론

침입대응시스템은 침입을 인식한 후, 공격행위를 기록하거나 공격에 대항하는 시스템을 말한다. 이와 같이 침입탐지와 그에 대한 대응기술은 서로 밀접한 관계에 있고, 위협 방어 측면에서도 중요한 기술이지만 아직까지 많은 연구들이 이루어지지는 않았다. 초기의 침입대응시스템으로서의 경보 시스템은 현재까지 대다수의 대응 시스템이 취하고 있는 형태로서 탐지정보를 관리자에게 전송해주거나 단순한 보고기능을 제공하며, 긴급을 요하는 경보일 경우 이메일 또는 이동 전화 등을 통한 서비스를 제공하기도 한다. 해당 공격을 저지하고 피해시스템을 복구하는 등의 작업등은 대부분이 시스템 관리자들이 직접 나서서 적절한 대응기술을 선택하여 수행되도록 하는 수동 또는 반자동 대응 방식을 취하고 있는데, 이는 자동대응기법과 비교할 때 고비용의 문제와 같은 대응을 수행하였다 하더라도 관리자의 능력 또는 대응 시간에 따라 그 결과가 서로 달라지기 때문에 이러한 여러 대응변수에 일률적으로 대처하기가 어렵다.

이에 반해, 자동대응시스템은 침입행위에 대한 대응기능을 프로그램화하여 시스템이 적절한 대응을 수행하도록 하는 시스템을 말한다. 현재시점에서의 자동대응시스템은 의사결정 테이블을 사용하여 공격이 발생하면 해당되는 테이블에서 대응방법을 찾아 수행하도록 하는 간단한 대응 메커니즘이다. 이 경우 침입과 대응이 정적 매핑에 의해 연결되므로, 최적의 대응을 이루기 위해서 모든 가능한 상황에 대해서 정적테이블을 유지해야만 한다. 그러나 모든 일어날 수 있는 상황을 알지 못할 뿐만 아니라 네트워크의 규모가 커질 경우 정적테이블을 일일이 생성하는 작업은 매우 번잡한 일이 아닐 수 없다.

이 상의 문제점 외에도 자동 침입대응 시스템에서 해결해야 할 여러 가지 문제점 및 해결사항들이 아래와 같이 존재한다.

- 방대한 양의 경보 처리능력 : 침입탐지시스템에서 생성한 방대한 양의 경보 중에서 침입대응시스템은 심각한 수준의 침입과 위험한 공격자를 구별해낼 수 있어야 한다. 이를 통해 대응의 소요시간을 단축시키고 중복대응의 가능성을 배제시킬 수 있어야 한다.
- 침입탐지의 오판 가능성 인지능력 : 현 침입탐지기술을 볼 때 오판의 가능성이 늘 존재하며, 이 경우 사용자들에게 부정적인 영향을 끼칠 수 있기 때문에 소극적인 대응이 이루어지는 이유가 되기도 한다. 또한 오판으로 인해서 불필요한 대응비용이 추가로 부담될 수 있다는 가능성을 배제할 수 없다.
- 주변상황에 따라 대응 및 방어강도 조절능력 : 인터넷의 활성화로 네트워크의 사용범위가 확대되면서 대규모네트워크에서 통일화된 대응 정책 적용이 필요하다. 같은 공격이 들어왔다 하더라도 현재의 네트워크 상황에 따라 다른 수준의 대응 및 방어 강도를 허용함으로써 좀더 효율적이고 정밀한 보안이 이루어질 수 있도록 해야 한다.

본 논문에서는 이상의 문제점들을 고려하여, 자동화된 침입대응이 가능하도록 하는 침입대응 시스템 및 그 메커니즘에 대해서 설명하고자 한다. 중복대응을 막고, 침입탐지센서의 정확도에 근거하여 가능한 대응집합을 설정함으로써 대응의 부정적인 영향을 감소시키고자 하였으며, 공격 강도를 결정하여 대응의 강도 및 기법을 선택하여 기술적 효율성 및 비용의 적절성을 고려하고자 하였다.

2. 자동화된 침입대응 시스템

2.1 시스템 구조

아래의 그림 1은 본 논문에서 제안하는 자동 침입대응시스

템의 구조도로서 계층구조를 가지며, 크게 대응계층과 조정계층으로 구분할 수 있다.

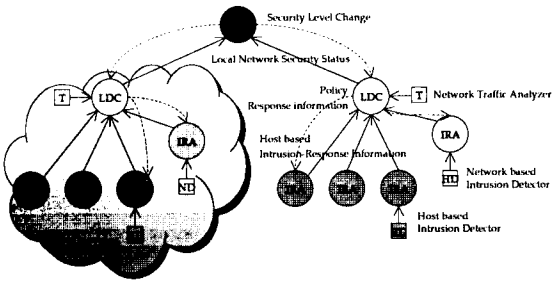

그림 1. 계층구조의 분산 자동침입대응시스템

대응계층에서는 침입탐지센서로부터 받은 이벤트를 분석하여 최적의 대응기법을 자동적으로 생성하여 수행하는 IRA(Intrusion Response Agent)가 위치하며, 조정계층에서는 다수의 IRA에서 보내준 정보를 통합·분석하여 각 보안영역에 대해 전역수준의 방어전략 수립이 가능하도록 하는 LDC(Local Domain Coordinator)와 GDC(Global Domain coordinator)가 위치한다.

2.2 구성 요소

(1) IRA(Intrusion Response Agent)

침입탐지센서로부터 탐지정보를 받아 공격에 따른 대응전략을 세우고, 실제로 대응행위를 수행하는 역할을 담당한다. 탐지정보를 분석하고 적절한 대응전략을 탐색하는 과정에서 몇 가지 인공지능 기법이 사용되며 이러한 과정에서 추출된 대응전략은 대응자(responder)에게 전달되어 자동대응이 이루어지도록 한다. 탐지정보와 수행된 대응결과 정보는 해당 관리영역의 LDC에게로 전달되어 대응 평가 또는 대응 및 방어 수위를 결정하는데 있어서 중요한 자료로 사용된다. 아래는 IRA에서 수행하는 주요 기능 중 몇 가지 기능에 해당한다.

◦ 침입탐지정보의 불확실성 제거
- 방대한 양의 경보에서 실제 공격만을 분리
- 새로운 공격의 시작인지, 진행중의 공격인지를 판단

이러한 불확실성의 제거과정을 통해 중복대응의 가능성이 줄어들게 된다.

◦ 검증된 탐지정보로부터 적절한 대응 기법 추출
- 공격자의 위치에 따라 대응 위치 및 컴포넌트 결정
- 대응컴포넌트와 공격방법에 따라 대응 전략 결정

대응기법의 추출 시 공격의 대상 시스템 등의 중요도 등을 고려하여, 대응 비용 및 피해비용 등을 산출하여 좋은 보안 시스템의 요건(기술과 비용 측면 고려)을 만족하도록 할 수 있다.

(2) LDC/GDC(Local/Global Domain Coordinator)

LDC는 하나의 보안 관리영역별로 위치하며, 해당 영역에서 탐지정보와 대응 결과 정보를 수집하여 현 관리영역의 방어 및 대응 수위를 결정하는 역할을 담당한다. LDC에서 결정된 방어 수위는 상위모듈인 GDC에게 전송되며, GDC는 이러한 LDC의 정보들을 통해 향후 일어날 수 있는 위협들을 제거함으로써 좀 더 안전한 보안 관리가 이루어지도록 해주며 통일화된 보안관리가 가능하도록 도와준다. 아래의 다양한 분석엔진들을 통해 관리영역의 경보 정보들을 참조하여 다양한 각도에서의 분석을 통해서 대응 수위가 결정될 수 있다.

◦ 공격 근원지 분석 엔진(Source Analysis Engine)
- 경보의 공격 근원지를 분석을 통해서 외부 또는 내부 공격이 주를 이루는지, 또는 위험한 공격자가 계속해서 공격을 수행하고 있는지를 분석

◦ 공격 대상 분석 엔진(Target Analysis Engine)
- 중요 정보시스템을 목표로 하는 공격 등이 얼마나 발생하였는지를 진단

◦ 경보 트래픽 분석엔진(alarm Traffic Analysis Engine)
- 전체 발생한 경보의 트래픽을 분석하는 엔진으로, 평상시보다 경보 트래픽의 증가했다는 의미는 많은 공격 시도 및 공격 행위 수행이 있었다는 사실을 유추할 수 있다.

◦ 공격위험도분석엔진(Attack severity Analysis Engine)
- 전체 발생 경보 중에서 공격위험도가 매우 높아 심각하게 고려해야할 공격 등이 있었는지 분석

◦ 추론 엔진(Decision Engine)
- 각각의 다양한 분석엔진으로부터 분석결과를 받아 대응 수위를 결정하는 역할을 담당한다.

2.3 자동대응 메커니즘

좋은 보안시스템의 모델은 최소의 비용으로 최대의 보안효과를 줄 수 있어야 한다. 이는 탐지패턴의 개수만큼 대응의 가지수를 증가시키는 노력이 중요한 것이 아니라는 것을 말해주고 있다. 침입탐지시스템과 마찬가지로 자동 침입대응시스템 역시 기술적 효율성과 함께 비용의 적절성을 고려할 때 좋은 보안시스템의 요건을 충족시킬 수 있다. 따라서 본 논문에서 추구하는 자동 침입대응 모델은 원하는 수준의 정확성을 유지하는 반면 비용요소와 대응 수행 시 발생 가능한 부정적인 측면까지 고려함으로써 최선의 대응기법이 수행되도록 하는 것이다.

(1) 비용 요소 (Cost factor)

자동대응 결정에 영향을 줄 수 있는 비용 요소로서 대응 비용(Response Cost)과 손실 비용(Damage Cost) 그리고 역효과 예상 비용(penalty Cost)을 이야기할 수 있다[1,4].

◦ 손실비용 : 공격으로 인한 피해정도를 수치화한 값으로 공격대상 시스템의 중요도와 피해 범위 및 심각도에 따라서 측정이 가능하다.

◦ 대응비용 : 보안정책, 공격의 형태 및 대상에 따라서 수행가능한 대응 행위 수행을 수치화 한 값으로, 손실비용 및 대응 비용은 공격 대상시스템의 중요도 등을 고려하여 가변적으로 산정 될 수 있다.

◦ 역효과 예상 비용 : 해당 공격에 대한 대응 수행 시, 발생가능한 부정적인 측면을 측정하여 비용으로 계량화시킨다. 이 값이 작다는 것은 해당 대응을 수행하더라도 사용자들에게 다른 대응기술보다 좀더 적은 부정적인 영향을 미칠

수 있다는 것을 뜻한다. 이 값의 산정은 침입탐지센서의 신뢰도에도 영향을 받는다.

이와 같은 비용은 해당 공격에 대해서 공격으로 인한 피해정도, 공격에 가능한 대응기술 집합 그리고 대상 기술들을 수행하였을 경우 발생가능한 역효과들에 대해서 미리 충분히 고려한 후 결정되어야 한다. 또한 이러한 비용요소들은 자사의 조직에 따라 조정이 가능하며 이는 사전에 미리 정의되어 있어야 한다.

(2) 대응 결정

비용기반의 대응 결정은 공격의 피해형태 등을 결정함으로써 대응 전략을 수립하고 탐지 정보의 신뢰도에 따라 대응의 부정적인 측면을 조절함으로써 최선의 대응이 선택되도록 한다.

대응 전략의 수립단계에서는 대응 절차에 따라서 제1대응, 제2대응, 제3대응 전략 도출이 가능하다. 제1대응에서는 주로 관리도구 또는 관리자에게 알림 기능을 제공하고, 제2대응은 해당 공격에 대한 대응 전략을 그리고 제3대응은 공격으로 인한 피해 발생 시 복구절차의 계획을 담고 있다.

이의 전략과 절차는 공격이나 상황에 따라 유동적 변화가 가능하다. 제2대응에서 공격에 대한 대응 전략은 대응의 부정적인 측면을 충분히 고려하여 대응 기술이 선택되도록 한다.

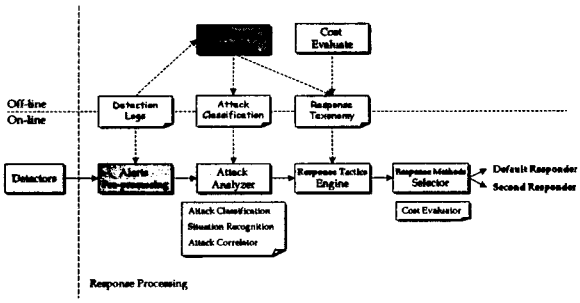

그림 2. 탐지에서 대응까지의 과정

위의 그림 2는 탐지에서 대응까지의 과정을 설명하고 있다. 복수 침입탐지센서로부터 이밴트 수신 시 경보의 전처리기로부터 경보 클러스터를 생성하는데, 경보 클러스터란 동일한 공격에 의해 생성된 경보의 집합을 의미한다. 이 과정에서 ongoing 공격과 새로 진행한 공격을 구분하여 중복 대응 수행을 방지하도록 한다.

공격 분석기는 공격에 대한 정확한 정보를 바탕으로 목적지 계층, 근원지 계층, 공격 유형 등의 정보를 이용하여 협력 공격 및 분산공격 등의 공격상황을 분석하여 대응 전술 수립 시 이에 대한 상태 정보도 함께 반영되도록 한다. 대응 전술 엔진은 공격 강도와 피해유형 및 정도를 분석하여 최선의 대응전략이 수립되도록 하며, 이 과정에서 제1대응, 제2대응 그리고 제3대응 계획이 세워진다. 대응기술 선택기는 대응 수행여부를 결정하고 탐지센서의 신뢰도에 기반하여 대응의 부정적인 면을 평가하여 대응기술이 선택되도록 한다. 대응기술 선택 시 만일, 대응비용이 피해비용보다 클 경우에는 경우에 따라서 대응을 수행하지 않거나 로깅 등의 소극적 대응을 수행하도록 할 수 있다.

반대로 대응 비용이 클 경우에는 공격에 대한 적절한 대응기술이 선택되어야 하며 이는 탐지정보의 신뢰도에 따라 대응의 부정적 측면과 공격의 강도에 따라서 결정된다.

표 1. 대응 조건

[1] No action : DCost(e) if DCost(e) < RCost(e) then No-action or logging
[2] Reaction : RCost(e) - elDCost(e) if DCost(e) ≥ RCost(e) then minimal PCost in chosen

대응 기술이 선택되면 실제 대응기능을 수행하는 대응자를 트리거하여 대응이 수행되도록 한다.

3. 결론

좋은 보안 시스템은 최소의 비용으로 최대의 보안효과를 창출할 수 있어야 한다. 본 논문에서는 비용산출모델을 자동대응 기법에 적용하여 기술적 효율성과 함께 비용의 적절성을 고려해 좋은 보안시스템의 조건을 충족시키도록 하였다.

먼저, 자동대응이 용이하도록 특정기준에 따라 대응기법을 분류하여, 공격의 강도 및 유형에 따라 적절한 대응 절차와 대응 전술이 수립되고 공격의 피해유형과 정도를 결정함으로써 최적의 대응기능이 수행되도록 한다.

공격의 진행결과에 따라서 다양한 대응기술들이 선택될 수 있는데 향후 연구로는 공격의 진행결과의 대응시간에 따라 차별적인 대응기법이 선택되도록 하여 더욱 정확한 대응기법이 수행되도록 하고자 한다.

참고문헌

[1] M Schultz, E. Eskin, E. Zadok and S. Stolfo, "Toward Cost-Sensitive Modeling for Intrusion Detection and Response", ACM CCS Workshop on Intrusion Detection Systems, 2000.

[2] Dipankar Dasgupta and Fabio A. Gonzalez, "An Intelligent Decision Support System for Intrusion Detection and Response", MMM-ACNS, May 21-23, 2001.

[3] Barrus, J. and Rowe, N.C., "A Distributed Autonomous-Agent network-Intrusion detection and Response system", Proceedings of the 1998 Command and Control Research and Technology Symposium, Monterey CA, June-July 1998.

[4] Thomas Toth and Christopher Kruegel, "Evaluting the Impact of Automated Intrusion Response Mechanisms", 18th Annual Computer Security Applications Conference, December 2002.