효율적인 IDS를 구성하기 위한 공격트리의 반복적 개선 기법

허 웅, 권호열
강원대학교 컴퓨터정보통신공학과
전화 : 033-250-6389 / 핸드폰 : 011-9929-2425

An Iterative Attack Tree Construction Scheme for Intrusion Detection System

Woong Hur, Ho-Yeol Kwon
Dept. of Computer & Inform. Comm. Engineering, Kangwon National University
E-mail : soul@mail.kangwon.ac.kr

Abstract

This paper proposes a efficient way to use Database that is constructed about attack-pattern.

For IDS that activate confrontation, we reconstruct by Layered Attack Tree after constructing attack-pattern by Attack Tree.

And then this paper has designed IDS that Layered Attack Tree is applied, verified them.

I. 서론

인터넷의 확장에 따라 국내외 해킹 사고 발생률이 급격하게 증가하고 있다. 인터넷을 통하여 해킹 기술에 대한 접근이 더욱 용이해지고 네트워크 침해 기법이 더욱 고도화되어 기업 정보시스템 관리자의 정보량 및 작업량이 매우 커지게 되었으며, 이에 따라 국내외의 정보 보호 업체에서는 보다 안전하고 효율적인 보안을 위한 해결책으로 네트워크 및 시스템에 대한 공격 패턴의 데이터베이스 작업 및 IDS (Intrusion Detection System)의 개발에 힘쓰고 있다. 현재 IDS관련 연구에서는 시스템 자원의 보호에 있어서 보호할 파일을 미리 설정하여 접근 제어를 수행하고 있으나 [1] 사용자의 편의와 IDS로 인한 시스템의 부하를 줄이기 위해 가변적 모니터링을 위한 연구가 요구된다.

본 논문에서는 각종의 공격 패턴을 수집하여 구축되는 데이터베이스의 자료를 보다 효율적으로 IDS에 적용하기 위하여 이미 수집된 공격 패턴의 데이터베이스를 관리하기 위한 방법으로 제안되고 있는 Attack Tree를 분석하였으며[2], 이를 지속적으로 정제하기 위한 방법으로 Layer 기반의 Attack Tree로서의 재가공을 제안한다. 또한 IDS에의 적용을 통하여 Layer 기반 Attack Tree의 이점을 검증한다.

II. 연구 배경

2.1 IDS (Intrusion Detection System)

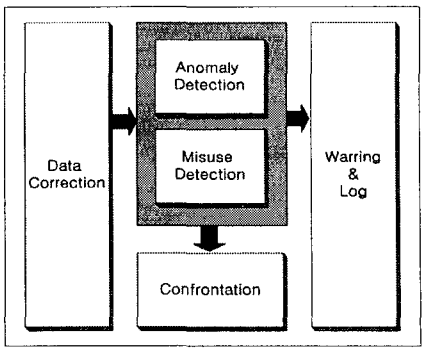

그림 3 IDS의 개념적 구성

IDS는 시스템이나 네트워크 침입을 즉각적으로 탐지하고 대처하며 보고하기 위한 자동화된 시스템으로서 침입자에 의한 불법적인 사용 및 합법적인 사용자에 의한 오용이나 남용을 탐지하는 것을 목적으로 한다. IDS의 개념적 구성은 그림 1과 같다.

현대의 침입 탐지 시스템은 경고 및 로그파일을 남기는 차원을 넘어서 보다 능동적인 대처를 할 수 있는 방향으로 발전하고 있다.

2.2 Attack Tree

정보 보안에 있어서 기존의 침입 사례에 대한 분석이라고 여겨짐에 따라 공격 패턴에 대한 데이터베이스화가 활발히 이루어지고 있다. 또한 이렇게 수집된 데이터베이스를 어떻게 구축하느냐는 방안으로 최근 Attack Tree Modeling의 방법이 제시되고 있다.

Attack Tree는 기본적으로 And와 Or관계로 구성되며 간략한 표현은 그림 2 및 그림 3과 같다.

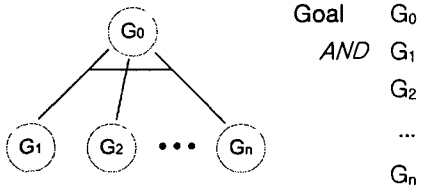

그림 4
And-decomposition

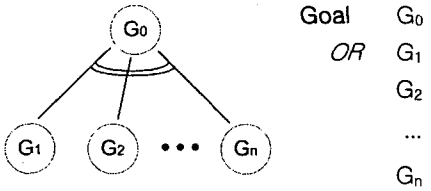

그림 6 Or-decomposition

G_0를 최종 목표라고 볼 때, G_0에 도달하기 위해서 And-decomposition의 경우에는 G_1, G_2, ...,G_n 모두를 실행해야 하는 반면 Or-decomposition의 경우에는 G_1, G_2, ..., G_n중 하나만을 실행하면 G_0에 도달할 수 있으며 이러한 관계는 복합적으로 나타날 수 있다. 또한 And, Or 연산을 통하여 Tree의 확장을 이룰 수 있다.

2.3 Refinement of Survivable System

보안 시스템의 개선을 위한 방법론으로 새롭게 제안되고 있는 방법으로 Architectural Refinement Process가 있다.[3] 이는 소프트웨어 개발 방법론으로 유명한 나선형 모델을 보안 시스템의 개선에 적용시킨 방법론으로, Network-Based Attacks, Application-Based Attacks, Data-Centered Attacks에 대해서 지속적으로 Survivability Planning, Usage Modeling, Intrusion Modeling, Survivability Risk Analysis를 수행하며 절차적 구성은 그림 5와 같다.

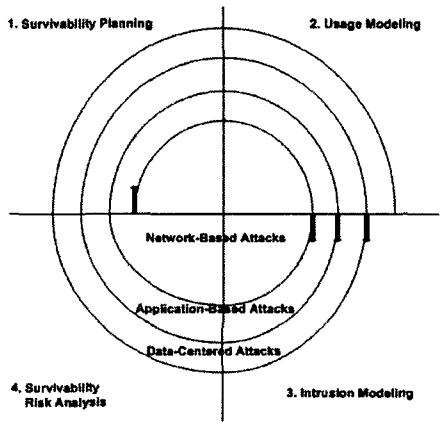

그림 5 Architectural Refinement Process

III. Layer 기반의 Attack Tree

Tree 구조를 통하여 공격 패턴의 데이터베이스를 구성할 경우 관리와 분류가 편해진다는 장점이 있으나 지속적인 정제작업을 위한 나선형 모델의 적용이 힘들다는 한계가 있다. 나선형 모델의 경우 단순한 Tree 구조에 기반을 둔 정제 작업이 이루어지는 것이 아니라 규정에 따라 계층적으로 분류하여 연속적인 정제 작업을 수행하기 때문에 Attack Tree에서 나선형 모델의 정제 작업을 위해 Layer 개념을 적용한 Layered Attack Tree를 제안한다. Layered Attack Tree의 경우에는 depth개념이 아닌 Layer의 개념으로 구간을 결정하며 한 Layer에는 2 이상의 depth를 갖는 Tree 구조의 일부분이 존재할 수 있다. 정제작업은 각각의 Layer를 기반으로 이루어지며 Attack Tree의 관점에서 서로 다른 depth에 존재하는 공격이라 해도 동일한 Layer에 존재하는 경우에는 Tree에서의 depth를 같은 등급으로 간주한다.

그림 6에서 보이는 일반적인 Attack Tree의 경우, depth 3에 해당하는 Tree를 보이고 있으며 depth별로 분류할 경우 [G_0], [G_1, G_2, G_3], [G_4, G_5, G_6, G_7]의 세 개 구간으로 나눌 수 있다. 반면에 그림 7에서 보이는 Layered Attack Tree의 경우에는 기본적으로 그림 6

의 Attack Tree와 같은 형태를 가지고 있으나 Layer 별로 분류할 경우 [G_0], [G_1, G_3], [G_2, G_5, G_7], [G_4, G_6] 의 네 개 구간의 분류가 가능해진다.

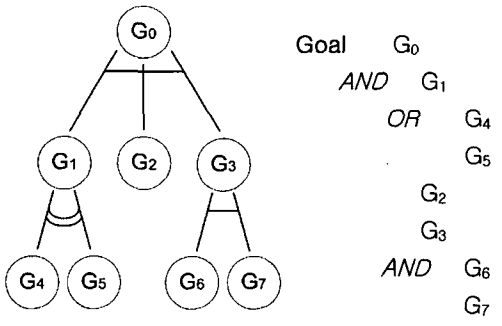

그림 6 Attack Tree

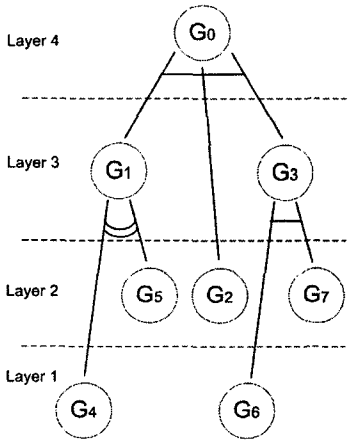

그림 7 Layered Attack Tree

Ⅳ. Layered Attack Tree의 IDS 적용

4.1 IDS 적용에서의 Layer 분류

Layer 분류	해당 시스템 자원
Data Layer	File, Device, …
System Layer	Application, 바이너리 컴파일러, Script 실행기, …
Network Layer	telnet, http, ftp, mail, ping, …

표 1 Classified Attack Tree Layer

본 논문에서는 IDS에 적용하기 위한 Attack Tree의 Layer를 사용자가 접근할 수 있는 자원의 종류에 따라 Data Layer, System Layer, Network Layer의 세 개 Layer로 분류한다. Layer의 분류는 접근 경로 및 자원의 안정성 요구 정도, 차후의 정제작업을 위한 경계의 명확성을 기준으로 이루어졌으며 표 1은 각 Layer에 해당하는 시스템 자원을 정리하고 있다.

4.2 Layered Attack Tree를 적용한 IDS의 설계

IDS의 유용성에도 불구하고 IDS 자체가 지나치게 많은 로그를 생성하여 그 효율성을 떨어뜨리는 경우가 있다. 여러 이벤트에 대한 로그의 생성이 침입 시도를 기록하고 보안 대책을 수립하는데 도움이 되는 것은 사실이지만 일일이 분석하기 힘들 정도로 많은 로그의 생성은 비정상 행위와 오용을 구분하기 힘들게 한다. IDS에 대한 Layered Attack Tree의 적용은 이벤트의 기록에 목적이 있는 것이 아니라 불법적인 사용으로 추측되는 이벤트가 발생했을 경우 그것을 기반으로 시도될 수 있는 더욱 큰 공격에 대해 예상을 목표로 한다. 따라서 특정 공격이 있은 후 다음으로 예상되는 공격에 대한 감시의 강화 및 보안 레벨의 조정으로 보다 적극적인 대응이 가능해진다.

그림 8의 시나리오는 임의의 사용자가 서버에 스크립트 파일을 전송한 후 실행을 시켜 서버가 오동작을 일으키게 하는 예를 보이고 있다. 스크립트 파일을 실행할 경우 버퍼 오버플로우를 통해 관리자 권한을 획득하여 보호되어야 하는 파일에 접근하는 경우와 샌드메일과 같이 부당한 네트워크 자원을 이용하고자 하는 경우 관리자는 미리 해당 Layer에 따라 IDS를 적절하게 설정하여 위험의 방지와 사용자의 편의라는 두 가지 목적을 만족시킬 수 있다. 결과적으로 악의적일 수 있다고 판단되는 스크립트의 실행이 있을 경우, 네트워크 Layer에 해당하는 네트워크 자원의 사용은 허용하되 데이터 Layer에 해당하는 시스템 내 파일에는 직접적인 접근을 할 수 없도록 설정하며 이는 추후의 업데이트 정보에서도 그대로 유지된다.

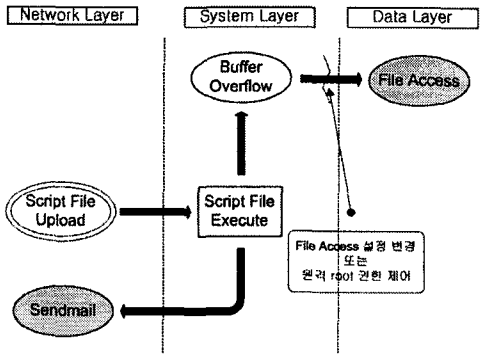

그림 8 Scenario of Script File Execute

4.3 Layered Attack Tree를 적용한 IDS의 구현

(1) IDS 적용 시나리오

그림 9는 시스템 자원을 고갈시키는 시스템 내부에서의 DoS (Denial of Service) 공격이 새로운 공격을 위한 사전 공격으로 사용되는 예를 보이고 있다. Race Condition은 프로그램 실행시 생성되는 임시파일의 접근 권한을 이용하여 해당 파일에 대해 관리자의 권한으로 접근하도록 하는 해킹 기법을 말한다. Race Condition을 피하는 방법으로 여러 프로그래밍 규칙들이 존재하나, 경우에 따라 그러한 규칙이 통용되지 않는 경우가 존재할 수 있으며 강한 DoS 공격이 있다면 공격자가 보다 쉽게 Race Condition이 적용될 수 있는 시스템의 취약점을 발견할 수 있다. 그림 9의 공격은 DoS 공격과 Race Condition이 System Layer에 해당하며 파일에 대한 Root 권한의 접근은 Data Layer에 해당한다. 본 논문에서는 DoS 공격의 발생시 Race Condition의 시도를 체크하는 것으로 Layered Attack Tree를 시험한다.

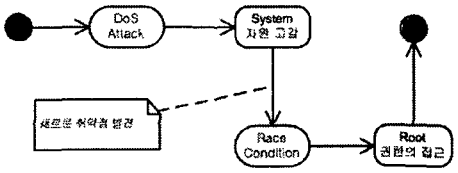

그림 9 Extends of DoS Attack

(2) IDS의 구현

DoS로 예측되는 상황이 발생한 경우 IDS는 즉각적으로 Race Condition을 감시하기 시작한다. Race Condition에 대한 감시는 DoS 공격이 차단되는 시점까지 지속되며 도중에 Race Condition이 발생한 경우에는 기존의 설정에 따라 이벤트를 발생시키게 된다. 그림 10은 Race Condition을 감시하는 시스템의 구성도를 나타낸다. DoS의 발생은 IDS의 기본적인 기능으로 존재하는 '프로세스에 대한 감시'를 통하여 감지하며 Race Condition의 감시는 해당 임시파일의 변화를 추적하여 이루어진다.

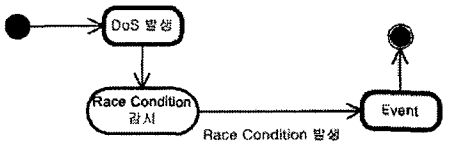

그림 10 시스템 구성도

V. 결론 및 향후 연구

시스템 보안에 있어서 가장 중요한 것은 주기적인 패치작업이라고 할 수 있으나 패치를 실시간으로 수행하는 것은 사실상 불가능하기 때문에 모든 시스템은 잠재적인 위험에 노출되어 있다. 따라서 백신 프로그램과 마찬가지로 주기적인 자동 업데이트가 가능한 IDS의 도입은 매우 중요하다.

본 논문은 공격 패턴에 대해 구축한 데이터베이스를 Layered Attack Tree로 재구성한 후 IDS로 하여금 추후의 공격을 예측하도록 하여 관리자의 모니터링을 돕고 설정에 따라 즉각적인 대응을 할 수 있는 방안을 제시하였다. 새로운 공격패턴이 발견되어 IDS에 추가되었을 때에도 관리자가 기존에 설정해놓은 Layer 마다의 대응방침에 따라 자동으로 반응할 수 있기 때문에 보다 능동적인 보안 시스템의 구축이 이루어질 수 있을 것으로 기대한다.

이러한 관점에서 향후 과제로는 다양한 공격에 대응하기 위해 보다 세분화된 Layer에 대한 연구와 데이터베이스 업데이트의 관점에서 Layered Attack Tree를 지속적으로 정제해 나가가는 부분에 대한 연구가 기대된다. 또한 현재의 IDS에 Layered Attack Tree를 적용하는 것도 IDS 업체들의 발전을 위하여 필수적인 연구가 될 수 있을 것이다.

참고문헌

[1] Philippe Biondi, "LIDS 1.0 Specifications Version 1.0", http://www.lidp.org, 2001.1

[2] Andrew P. Moore, Robert J. Ellison, Richard C. Linger, "Attack Modeling for Information Security and Survivability", CMU/SEI, March. 2001.

[3] Robert J. Ellison, Andrew P. Moore, "Architectural Refinement for the Design of Survivable Systems", CMU/SEI, October. 2001.

[4] 한국 정보 보호 진흥원, "국외 침입탐지 시스템 제품 동향", 2001. 2.

[5] 한국 정보 보호 진흥원, "실시간 침입탐지기술"

[6] 서의성, "Race Condition을 이용한 Exploit", Security.KAIST, 1998.8.