계층적 패킷분석에 기반한 침입탐지 및 대응시스템

지정훈*, 남택용*, 손승원*

*한국전자통신연구원, 네트워크보안연구부

Intrusion Detection and Response System using Hierarchical Packet Analysis

Junghoon Jee, Taekyoung Name, Sungwon Sohn

*Network Security Department, ETRI

요 약

기존의 보안시스템은 각 기관의 로컬네트워크에 설치되어 해당 도메인으로 들어오는 트래픽에 대한 침입탐지에 의한 침입차단이 주된 역할이었다. 최근에는 침입자의 우회공격 및 DDoS 와 같은 공격의 증가로 이러한 시스템의 효용성이 크게 저하되고 있다. 본 논문에서는 침입자의 공격에 대하여 보다 적극적이고 효율적인 대응을 위하여 계층적인 패킷분석에 기반한 침입탐지 및 대응시스템을 제안한다. 계층적인 패킷분석을 위하여 가입자네트워크에서는 세션단위의 정보분석을 수행하고, 백본네트워크에서는 패킷단위의 정보분석을 수행한다. 네트워크도메인간에 이러한 정보교환을 통해서 침입탐지 및 역추적을 수행한다. 본 논문에서는 해당 시스템의 전체구조 및 각 기능구조를 보이며, 각 기능구조간의 동작구조를 보인다. 본 시스템을 통하여 침입자의 새로운 공격유형에 대한 탐지 및 대응이 가능하며, 침입사례의 조기발견을 통하여 네트워크의 안정성을 높일 수 있다.

I. 서론

기존의 보안시스템의 대표적인 것으로는 침입탐지시스템과 침입차단시스템을 들 수 있다.

침입탐지시스템은 호스트 혹은 네트워크상에서 발생하는 각종 사건들을 종합, 분석하여 침입자에 의한 침입 활동을 발견하고 이를 관리자에게 통보하거나 적절하게 대응하는 시스템이다. 침입탐지시스템의 종류에는 호스트단위에 설치되어 각 호스트에 대한 침입만을 탐지하는 종류의 호스트기반 침입탐지시스템이 있으며 서브네트워크 전체에 대한 감시를 수행하여 해당 서브네트워크상의 침입을 발견, 통보하는 네트워크기반의 침입탐지시스템이 있다[1][2].

침입차단시스템은 일반적으로 네트워크 방화벽이라고 불리며 네트워크와 네트워크 사이에 위치하여 네트워크간의 통신 연결을 선별적으로 허가 혹은 불허하는 역할을 통해서 특정 네트워크 혹은 호스트에 대한 접근 제어를 수행할 수 있는 시스템이다[3]. 방화벽은 패킷필터링방식의 네트워크레벨 방화벽과 프락시방식의 응용레벨방화벽, 그리고 이들 두가지 방식이 지닌 장점을 모두 갖춘 Stateful inspection 방식의 방화벽으로 구분된다.

상기의 침입탐지시스템과 침입차단시스템은 초창기에 독립적으로 운용되기도 했지만, 최근에는 대개 중앙의 관리시스템을 통하여 연동하거나 시스템상호간에 API를 규정하여 상호연동하도록 하여, 외부의 침입에 자동적으로 대응할 수 있도록 구성하고 있다[4].

하지만, 이러한 기존의 보안시스템은 외부의 공격으로부터 내부네트워크만을 보호하는데 초점을 두고 있다. 그 결과 침입자가 여러 네트워크를 경유하여 목적 호스트를 침투하는 우회공격[5] 및 여러 네트워크에 산재해있는 에이전트를 이용한 DDoS[6] 등의 공격에 대하여 대처하기 어려운 상황이다.

본 논문에서는 이러한 문제점을 해결하기위하여, 계층적인 패킷분석에 의한 침입탐지 및 대응시스템을 제안한다. 계층적인 패킷분석을 위하여 가입자네트워크에서는 세션단위의 정보분석을 수행하고, 백본네트워크에서는 패킷단위의 정보분석을 수행한다. 네트워크도메인간에 이러한 정보교환을 통해서 침입탐지 및 역추적을 수행한다. 본 논문의 구성은 다음과 같다. 2장에서는 본 시스템의 전체구조에 대하여 기술한다. 3장에서는 각 네트워크에서 시스템구조와 각각의 기능요소를 살펴본다. 4장에서는 본 시스템의 동작구조를 보이며, 5장에서 결론을 맺는다.

II. 전체구조

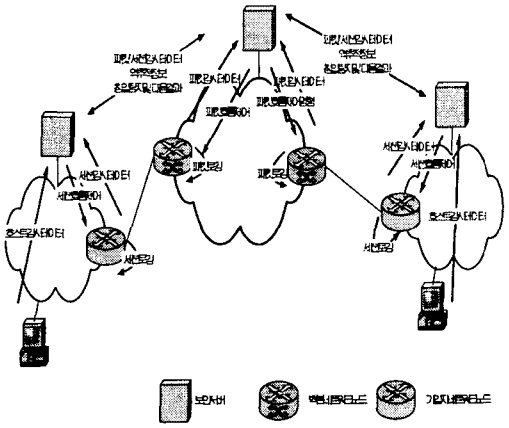
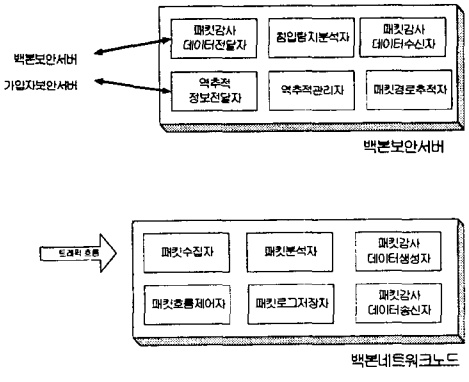


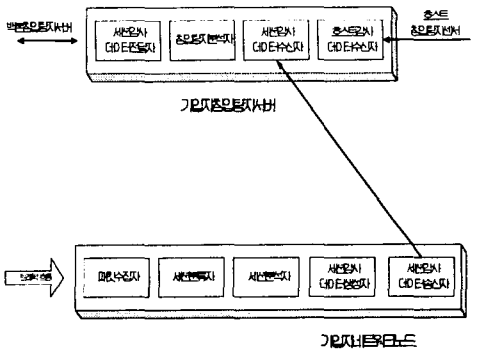
그림 1 전체구조

본 시스템은 그림 1과 같이 백본네트워크에 설치되어 전달되는 트래픽에 대하여 패킷수준의 정보를 수집하여 침입에 관련된 축약정보와 패킷로그정보를 관리하는 백본네트워크노드와, 가입자네트워크에 설치되어 전달되는 트래픽에 대하여 세션수준의 정보를 수집하여 침입에 관련된 축약정보와 세션로그정보를 생성하는 가입자네트워크노드와, 각 네트워크에서 상기의 네트워크노드들로부터 침입에 관련된 축약정보를 전달받아 침입을 분석하며 인접한 네트워크간에 침입축약정보를 상호전달하여 침입을 판단하며, 침입의 판단결과 침입자의 세션 및 패킷의 경로를 추적하여 각 네트워크노드에서 해당 침입자의 세션 및 패킷의 흐름을 제어하는 보안서버로 구성되어있다.

III. 시스템구조



a. 백본네트워크시스템



b. 가입자네트워크시스템

그림 2 시스템구조

백본네트워크와 가입자네트워크에 설치되어있는 시스템의 기능구조를 보인다.

백본네트워크노드는 네트워크상에서 패킷을 수집하는 패킷수집자와, 수집된 패킷으로부터 침입에 관련정보를 분석하는 패킷분석자와, 분석된 패킷정보에 따라 패킷수준의 축약데이터를 생성하는 패킷감사데이터생성자와, 해당네트워크도메인상의 보안서버측으로 패킷감사데이터를 전달하는 패킷감사데이터송신자, 침입자의 패킷흐름을 제어하기위한 패킷흐름제어자와 패킷의 경로정보를 저장하기위한 패킷로그저장자로 구성되어있다.

가입자네트워크노드는 네트워크상에서 패킷을 수집하는 패킷수집자와, 수집된 패킷으로부터 응용서비스의 세션별로 분류하는 세션분류자와, 수집된 세션으로부터 침입관련정보를 분석하는 세션분석자와, 분석된 세션정보로부터 세션수준의 침입관련 축약데이터를 생성하는 세션감사데이터생성자, 해당네트워크도메인상의 보안서버측으로 세션감사데이터를 전달하는 세션감사데이터송신자, 침입자의 세션흐름을 제어하기위한 세션흐름제어자와 세션의 경로정보를 저장하기위한 세션로그저장자로 구성되어있다.

백본네트워크에 설치되는 백본보안서버는 패킷감사데이터수신자, 패킷감사데이터전달자와 침입탐지분석자, 역추적정보전달자, 역추적관리자와 패킷경로추적자로 구성되어있다.

- 패킷감사데이터수신자

해당 네트워크상의 여러 백본네트워크노드들의 패킷감사데이터송신자들로부터 패킷감사데이터를 수신한다.

- 패킷감사데이터전달자

인접한 네트워크와 패킷감사데이터 및 세션감사 데이터를 상호교환하여, 인접한 네트워크가 백

본네트워크일경우에는 패킷감사데이터를 상호 교환하며, 인접한 네트워크가 가입자네트워크일 경우에는 패킷감사데이터를 송신하며 세션감사 데이터를 수신한다.

- 침입탐지분석자

패킷감사데이터수신자와 감사데이터전달자로부터의 정보를 이용하여 침입을 분석 및 판단한다.

- 역추적정보전달자

인접한 네트워크상의 보안서버와 역추적관련정보를 전달한다.

- 역추적관리자

해당 네트워크도메인내의 역추적관련정보를 관리한다. 패킷로그저장자로부터 패킷의 경로정보를 전달받으며, 역추적에 따른 대응명령을 통하여 침입자의 패킷흐름을 제어한다.

- 패킷경로추적자

해당 네트워크도메인을 거쳐간 패킷의 경로정보를 관리한다. 도메인내의 여러 백본네트워크 노드들의 패킷로그지장자를 통하여 패킷의 경로정보를 전달받아 특정 패킷의 경로를 파악한다.

가입자네트워크에 설치되는 가입자보안서버는 세션감사데이터수신자, 호스트감사데이터수신자, 세션감사데이터전달자, 침입탐지분석자, 역추적정보전달자, 역추적관리자와 세션경로추적자로 구성되어있다.

- 세션감사데이터수신자

해당 네트워크상의 여러 가입자네트워크노드들의 세션감사데이터송신자들로부터 세션감사데이터를 수신한다.

- 호스트감사데이터수신자

해당 네트워크상의 여러 호스트들에 설치된 호스트침입탐지센서들로부터 호스트감사데이터를 수신한다.

- 감사데이터전달자

인접한 네트워크와 패킷감사데이터 및 세션감사 데이터를 상호교환하여, 인접한 백본네트워크측으로 세션감사데이터를 송신하며 패킷감사데이 터를 수신한다.

- 침입탐지분석자

세션감사데이터수신자, 호스트감사데이터수신자와 감사데이터전달자로부터의 정보를 이용하여 침입을 분석 및 판단한다.

- 역추적정보전달자

인접한 네트워크상의 보안서버와 역추적관련정보를 전달한다.

- 역추적관리자

해당 네트워크도메인내의 역추적관련정보를 관리한다. 세션로그저장자로부터 패킷의 경로정보를 전달받으며, 역추적에 따른 대응명령을 통하여 침입자의 패킷흐름을 제어한다.

- 세션경로추적자

해당 네트워크도메인을 거쳐간 패킷의 세션경로정보를 관리한다. 도메인내의 가입자네트워크 노드의 세션경로지장자와 호스트상의 호스트감사데이터를 통하여 세션 경로정보를 전달받아 특정 세션의 경로를 파악한다.

IV. 동작구조

백본 네트워크에 설치된 하나이상의 백본네트워크노드들에서는 전달되는 트래픽에 대해서 패킷수준의 분석을 수행한다. 해당 노드들에서 수집된 패킷감사데이터는 백본보안서버측으로 전달된다. 백본보안서버에서는 수신한 여러 패킷수준의 감사데이터를 종합하여 침입여부를 판단한다. 필요시, 백본보안서버는 인접한 가입자네트워크의 가입자보안서버측에 요청하여 세션수준의 감사데이터를 수신하여, 패킷감사데이터와 세션감사데이터를 종합하여 침입여부를 판단한다.

가입자 네트워크에 설치된 하나이상의 가입자 네트워크노드들에서는 전달되는 트래픽에 대해서 세션수준의 분석을 수행한다. 해당 노드들에서 수집된 세션감사데이터는 가입자보안서버측으로 전달된다. 가입자보안서버에서는 수신한 여러 세션수준의 감사데이터를 종합하여 침입여부를 판단한다. 필요시, 가입자보안서버는 인접한 백본네트워크의 백본보안서버측에 요청하여 패킷수준의 감사데이터를 수신하여, 세션감사데이터와 패킷감사데이터를 종합하여 침입여부를 판단한다.

다음에서는 백본네트워크에서 백본네트워크노드의 패킷처리에 따른 백본보안서버에서의 침입탐지과정을 보인다.

① 백본네트워크노드에 패킷이 도착한다.
② 도착한 패킷은 패킷수집자를 통하여 패킷분석자로 전달된다.
③ 패킷분석자에서는 해당 패킷의 정보필드를 분류하여, 각각의 필드를 분석한다.
④ 패킷분석자를 통하여 분석된 패킷정보는 패킷감사데이터생성자를 통하여 패킷감사데이터로 저장된다.
⑤ 패킷감사데이터생성자를 통하여 생성된 패킷 감사데이터는 패킷감사데이터송신자를 통하여, 백본보안서버의 패킷감사데이터수신자측으로 전달된다.
⑥ 패킷감사데이터수신자는 수신한 패킷감사데이터를 침입탐지분석자측으로 전달한다.
⑦ 패킷감사데이터전달자는 인접한 네트워크의

패킷감사데이터전달자 또는 세션감사데이터 전달자로부터 인접한 네트워크에서 수집된 감사데이터를 전달받아 침입탐지분석자측으로 전달한다.

⑧ 침입탐지분석자는 패킷감사데이터수신자와 패킷감사데이터전달자로부터의 정보를 종합하여 침입을 판단한다.

⑨ 침입의 발생이 확인되면, 침입탐지자는 역추적관리자에게 해당 침입에 대한 역추적을 요청한다.

⑩ 역추적관리자는 패킷경로추적자에게 해당 침입에 대한 패킷의 경로정보를 요청한다.

⑪ 패킷경로추적자는 백본네트워크노드들의 패킷 로그저장자측으로 패킷경로의 로그정보를 요청한다.

⑫ 패킷경로추적자는 수신한 로그정보를 기반으로 패킷의 경로를 확인하여 역추적관리자측에 알려 준다.

⑬ 역추적관리자는 해당침입의 역추적경로를 확인하여 역추적정보전달자를 통하여 인접한 네트워크측으로 전달한다.

⑭ 상기의 10 - 13 과정을 반복하여 침입자의 근원지를 파악하여, 해당 네트워크의 보안서버측에서는 세션흐름제어자를 통하여 침입자의 세션을 차단한다.

V. 결론

본 논문에서는 침입자의 공격에 대하여 보다 적극적이고 효율적인 대응을 위하여 계층적인 패킷분석에 기반한 침입탐지 및 대응시스템을 제안한다. 계층적인 패킷분석을 위하여 가입자네트워크에서는 세션단위의 정보분석을 수행하고, 백본네트워크에서는 패킷단위의 정보분석을 수행한다. 네트워크도메인간에 이러한 정보교환을 통해서 침입탐지 및 역추적을 수행한다. 본 시스템을 통하여 침입자의 새로운 공격유형에 대한 탐지 및 대응이 가능하며, 침입사례의 조기발견을 통하여 네트워크의 안정성을 높일 수 있다.

참고문헌

[1] David J. Marchette, "Computer Intrusion Detection and Network Monitoring : A Statistical Viewpoint,," Springer-Verlag New York, Inc., 2001

[2] J.Clark, et all, "Network Intrusion Detection," Aerospace technical report, 1998

[3] C. Hare and K. Siyan, "Internet Firewalls and Network Security," 2nd ed,, New Riders Publishing, 1996.

[4] "OPSEC The Industry's leading open, multi-vendor security framework," http://www.opsec.com

[5] F. Buchholz et al., "Packet Tracker," CERIAS Final Report, available at http://www.cerias.purdue.edu/tracceback/.

[6] C.E.R.T. (CERT). CERT Advisory CA-2000-01-Denial-of-service developments, Jan. 2000.