제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

커널 수준의 침입탐지를 위한 동적 침입탐지 규칙 변경기법의 설계

정보흥°, 김정녀
한국전자통신연구원
email:{bhjung, jnkim}@etri.re.kr

Design of Dynamic Intrusion Detection Rule Modification Technique for Kernel Level Intrusion Detection

Bo-Heung Chung°, Jeong-Nyeo Kim
Electronics and Telecommunications Research Institute

요 약

본 논문에서는 커널수준의 침입탐지를 위한 동적 침입탐지 규칙 변경 기법을 제안한다. 제안하는 기법은 침입탐지 규칙은 규칙타입, 프로토콜 타입, 패킷 헤더와 패킷 페이로드에 대한 검사를 수행하기 위한 규칙들로 세분화하여 LVR로 표현하고 이들 LVR이 계층적으로 구성된 IDRL로 관리한다. 침입탐지는 IDRL을 이용하여 수행하며, 규칙에 대한 변경은 변경된 규칙에 대한 LVR을 구성하고 LV를 이용한 포인터 변경을 이용하여 IDRL에 반영하는 방법이다. 제안하는 기법은 IDRL을 이용한 침입탐지와 탐지규칙의 변경을 IDRL에 최소한의 비용으로 수행하고, LVR을 이용하여 침입탐지 규칙을 디스크와 메모리에 동일한 형태로 저장 및 관리하여 탐지규칙 초기화 비용과 변경 비용을 최소화할 수 있다. 이를 통하여 보다 안전한 커널 수준에서의 네트워크 보안을 위한 효율적인 동적 침입탐지 규칙 변경을 지원할 수 있다는 장점을 가진다.

Keywords: LV, LVR, IDRL, Intrusion Detection System, Secure Operating System, Network Security

1. 서론

네트워크 환경 및 인터넷의 급속한 발전과 다양한 형태의 네트워크 공격 등으로 인하여 네트워크 보안에 대한 필요성이 점점 증가하고 있다. 이러한 환경에서 네트워크 보안을 위해 기존에 사용되던 침입탐지시스템, 방화벽 등은 내부자 침입이나 해킹, 새로운 공격기법에 대해서는 한계가 존재한다. 따라서 보다 안전한 커널 수준에서의 네트워크 보안기법에 대한 연구가 요구되어지고 있다.

커널 수준의 보안강화를 위해서는 일반적으로 인증과 접근제어 기법이 사용되며, 해킹 및 네트워크 공격에 대한 네트워크 보안을 위해서는 규칙기반의 침입탐지 기법이 사용된다. 따라서 커널 수준의 시스템 및 네트워크 보안을 효율적으로 수행하기 위해서는 이 두 가지 기법을 병행하여 사용할 수 있어야 한다. 또한, 최근의 공격도구의 자동화와 복잡한 공격기법의 증가로 인하여 침입탐지 규칙에 대한 신속한 변경 및 편리한 관리가 이루어져야 하며, 탐지규칙 변경 시 변경을 요청하는 관리자와 해커를 구분할 수 있도록 접근제어와 인증의 기법이 같이 사용되어야 한다. 특히, 모든 패킷에 대하여 침입탐지를 수행하여야 하며 동시에 탐지규칙이 변경되면 이를 신속하게 반영하여 탐지를 수행할 수 있어야 하며 변경을 위한 부하를 최소화 할 수 있어야 한다.

본 논문에서는 커널수준의 침입탐지를 위한 동적 침입탐지규칙(Intrusion Detection Rule) 변경기법을 제안한다. 동적 규칙변경이라는 것은 커널을 재 부팅하지 않고도 새로운 침입탐지 규칙을 이용하여 침입탐지 과정을 수행할 수 있는 것을 말한다. 본 기법은 침입탐지 과정에 가변길이 레코드의 링크드 리스트(LVR:Linked-list of Variable-length Record)로 구성된 침입탐지 규칙 리스트(IDRL:Intrusion Detection Rule List)를 사용한다. 탐지규칙의 변경에는 참조변수(LV:Look-up Variable)을 사용한다. LVR은 메모리와 디스크에 침입탐지 규칙을 동일한 형

태로 저장 및 관리하기 위한 자료구조 이다. 침입탐지 규칙의 변경은 추가된 침입탐지 규칙 LVR 작성 후 LV설정과 IDRL의 포인터 변경만을 수행하는 부분적 규칙변경을 수행한다. 이 과정에서 LV는 변경된 규칙 LVR을 IDRL에 반영할 위치를 설정하기 위해 사용된다. 탐지규칙 변경은 LVR 노드 추가, LV 설정, LVR 노드 연결, LV 설정해제 단계로 진행된다.

본 논문에서 제안한 기법은 부가적인 자료구조 없이 동일한 IDRL을 이용하여 탐지 및 탐지규칙 변경을 수행하여 규칙변경 및 침입탐지를 위한 관리비용을 최소화할 수 있다. 커널 초기화 시에는 메모리와 디스크에 동일한 형태로 저장 및 관리할 수 있는 LVR 자료구조를 통해서 침입탐지 규칙 초기화 비용을 최소화한다. 또한 부분적 규칙변경을 통하여 최소한의 비용으로 침입탐지 규칙 변경을 수행할 수 있으며, 탐지규칙 변경 중에 탐지과정을 멈추고 대기해야 하는 시간을 최소화한다. 따라서, 본 기법은 IDRL 관리비용, 탐지규칙 초기화 비용, 탐지규칙 변경 비용을 최소화하여 효율적인 동적 침입탐지 규칙변경을 지원할 수 있다는 장점을 가진다.

본 논문의 구성은 다음과 같다. 2장에서는 안전한 운영체제를 위한 기존 기법과 규칙 기반의 침입탐지 기법에 대하여 기술하고, 3장에서는 동적 침입탐지규칙 변경을 위해 필요한 자료구조 및 동적 규칙 변경과정에 대하여 기술하고, 4장에서는 결론 및 향후 연구과제에 대해 설명한다.

2. 관련연구

본 절에서는 네트워크 보안을 제공하기 위해 안전한 운영체제 구축을 위한 기법과 침입탐지 기법에 대하여 설명한다.

2.1 안전한 운영체제를 위한 기법들

안전한 운영체제를 지원하기 위하여 사용자 인증과 접근제어 기법이 일반적으로 연구되어져 왔다. 사용자 인증 기법은 네트워크 환경에서 사용자를 인식하기 위한 기법으로 ID/Password, 스마트카드, 생체 인식 등의 다양한 방법이 있다[]. 접근 제어 기법은 객체에 포함된 정보의 비밀성과 이러한 비밀성의 접근정보에 대하여 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제한하는 방법을 말한다. 이러한 접근제어 기법에는 신분 기반 접근제어(DAC), 강제적 접근제어(MAC), 역할기반 접근제어(RBAC)가 있다[]. RSBAC[], SELINUX[],FreeBSD[]와 같은 시스템에서 연구되어졌다. 또한, 최근에는 FreeBSD 기반의 ETRI SecuROS 시스템에서 DAC, MAC, RBAC을 모두 구현한 시스템도 개발되어졌다[].

2.2 침입탐지 기법

침입탐지 시스템은 내부 또는 외부의 침입으로부터 시스템 및 네트워크를 보호하기 위한 조작을 수행하는 시스템을 말한다. 이 시스템은 침입을 즉각적으로 탐지하고 대처할 수 있는 기술이 필요하며 이를 위해 침입탐지, 보고, 대응의 과정을 수행한다[]. 침입탐지 시스템은 데이터 소스를 기반으로 단일 호스트기반, 다중 호스트 기반, 네트워크 기반의 침입탐지 시스템의 3가지 형태로 분류된다. 또한, 침입모델 기반으로는 비정상(anomaly detection) 침입탐지 시스템과 오용탐지(misuse detection) 침입탐지 시스템으로 분류된다[]. 오용탐지 시스템은 시스템이나 응용 소프트웨어에서 알려진 취약점을 통하여 시스템에 침입할 수 있는 공격 행위들을 사전에 공격에 대한 정보를 가지고 탐지하는 시스템이다. 이 시스템은 일반적으로 규칙기반의 침입탐지를 수행하며 커널수준에서 구현하기에 쉽고 탐지율도 우수하다고 할 수 있다.

3. 동적 규칙변경 기법

본 절에서는 동적 규칙 변경을 위한 자료구조와 그 방법에 대하여 설명한다.

3.1 침입탐지 및 동적변경을 위한 자료구조

침입탐지에 사용되는 IDRL은 탐지규칙 데이터베이스(DRDB:Detection Rule DataBase)에 저장되며 규칙타입(RT:Rule Type), 프로토콜별 탐지규칙(PDR:Protocol Detection Rule) 자료구조와 패킷 헤더 검사규칙(PHCR:Packet Header Check Rule), 패킷 페이로드 검사규칙(PPCR:Packet Payload Check Rule)을 포함한 자료구조로 구분된다. 이를 그림으로 도식화한 것이 그림 1이다.

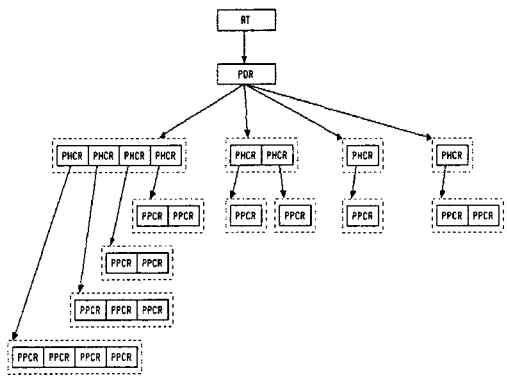

그림 1. DRDB내의 IDRL 구조

RT는 침입이 탐지된 후 어떠한 형태의 보고 또는 대응을 수행하는가에 따라서 결정되며 "alert, log, activate, dynamic" 등이 있다. 본 논문에서는 침입탐지 시 경보를 제공하는 'alert'타입을 지원한다. PDR은 패킷에 대한 침입탐지 시 TCP, UDP, ICMP, IP 프로토콜에 대한 침입을 검사하기 위한 자료구조이다. PHCR은 침입탐지시 패킷헤더에 대한 검사를 수행하는 규칙을 관리하는 자료구조이며, PPCR은 패킷 페이로드에 대한 침입탐지 검사를 위한 정보를 포함하는 자료구조이다. 이들 RT, PDR, PHCR, PPCR은 계층적인 순서를 가진다. 즉, RT는 PDR를 포함하고, PDR은 여러 개의 PHCR을 가지며, PHCR은 여러 개의 PPCR을 가지는 형태이다.

IDRL의 각 자료구조는 LVR로 관리 되며 LVR은 그림 2와 같이 next, count 필드를 가진다. LVR에서 next 필드는 레코드간의 연결상태를 관리하기 위하여 이용되며, count 필드는 하위에 연결된 자료구조의 개수를 관리하기 위하여 사용된다.

LVR의 각 노드들은 상위 LVR의 count 값에 의하여 연속적인 공간에 할당되며 next 포인터를 이용하여 연결된다. LV는 IDRL에서 현재 변경이 수행되고 있는 위치를 기록하기 위한 자료구조이며, 초기값은 NULL로 설정되고 변경 시에는 해당 PDR, PHCR, PPCH ID값이 설정된다.

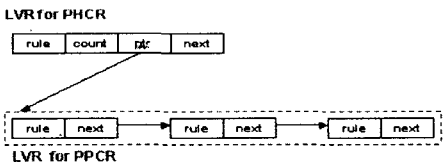

그림 2. LVR의 구조

3.2 침입탐지 규칙 초기화 및 탐지과정

탐지규칙 초기화는 DRDB로부터 IDRL을 메모리로 로딩하는 과정이다. 이 경우 디스크 I/O 시간과 같은 초기화 과정의 부하를 최소화하기 위하여 여러 개 블록 단위로 한꺼번에 디스크 접근을 수행한다. 즉, PDR 자료구조를 읽어서 각 프로토콜별로 하위에 연결된 PHCR의 개수가 저장된 count 필드를 이용하여 메모리를 한꺼번에 할당하고 이 할당된 크기만큼 디스크 접근을 수행한다. 따라서, 메모리에 로드된 PHCR은 연속적인 공간에 할당되며 마치 배열과 같은 조작이 가능하다. 또한, PHCR 각각의 레코드들간의 연결상태는 메모리 내에서 이루어지며 배열의 다음 인덱스에 해당하는 주소를 앞 레코드의 next 필드에 할당하면 된다.

침입탐지 과정에서는 메모리에 구성된 IDRL을 이용하여 RT에서부터 PPCR로 차례대로 순회하여 침입탐지를 수행한다.

IDRL을 DRDB로 저장하는 경우에도 RT에서부터 PPCR로 차례대로 순회하여 저장한다. 이때 RT와 PDR, PHCR, PPCR을 각각 분리된 디스크 공간에 저장한다. 그 과정은 RT와 PDR을 기록하고 PDR의 TCP 프로토콜에 연결된 PHCR을 count 필드 개수만큼 한꺼번에 기록하고 UDP, ICMP, IP 순으로 기록한다. PHCR을 기록함과 동시에 여기에 연결된 PPCR을 count 개수 만큼 기록한다.

3.3 침입탐지 규칙의 변경

동적 규칙변경이라는 것은 커널을 재 부팅하지 않고도 새로운 침입탐지 규칙을 이용하여 침입탐지 과정을 수행할 수 있는 것을 말하며 이를 위해 LVR과 LV를 사용한다. 탐지규칙 변경과정은 LVR 노드 추가, LV 설정, LVR 노드 연결, LV 설정해제의 단계를 통해 수행된다. LVR 노드추가 단계는 추가되거나 변경되는 탐지규칙에 대한 RT, PDR, PHCR, PPCR에 대한 LVR 노드를 생성하고 초기화한다. LV 설정 단계는 현재 변경이 이루어져야 할 IDRL에서의 위치에 대한 정보를 LV에 설정한다. 만일 LV가 설정되어 있고 탐지과정에서 이 위치 LVR노드를 이용하여 탐지를 수행하려고 한다면 변경이 완료될 때까지 침입탐지는 미루어진다. LVR 노드 연결 단계는 새로 생성된 LVR 노드를 LV에 설정된 IDRL 노드에 next 필드에 대한 포인터 조작을 통하여 삽입하거나 변경하는 단계이다. LV 설정 해제 단계는 이러한 모든 단계를 마치고 난 후 LV의 값을 초기값으로 바꾸어 미루어진 탐지과정이 계속 수행될 수 있도록 한다. 탐지규칙 변경과정에서 새로이 변경되는 탐지규칙에 대한 LVR 생성과정은 침입탐지 과정과 별도로 수행되고 IDRL에 대한 변경작업은 최대 3번의 포인터 조작을 통해 수행한다. 따라서, 침입탐지와 탐지규칙 변경을 동시에 수행하기 위한 부하를 최소화 할 수 있다.

4. 결론

본 논문에서는 커널수준의 침입탐지를 위한 동적 침입탐지규칙(Intrusion Detection Rule) 변경기법을 제안하였다. 제안된 기법은 IDRL을 이용하여 침입탐지를 수행하고 IDRL에 대한 초기화와 변경은 LVR과 LV를 이용하여 수행하는 기법이다. 또한, 제안 기법은 침입탐지와 규칙변경에 동일한 IDRL을 사용하여 관리비용을 줄이고, LVR과 LV를 통하여 IDRL 초기화 비용과 탐지규칙 변경을 비용을 최소화할 수 있다는 장점을 가진다. 따라서, 본 기법은 보다 안전한 커널 수준에서의 네트워크 보안기법으로 효과

적으로 사용될 수 있다. 향후 연구과제로는 네트워크 보안 유지 및 관리를 위한 보안정책과 상호연동 하여 침입탐지 규칙에 대한 변경을 수행하기 위한 방법에 대한 연구가 필요하다.

참고문헌

[1] Stephan Northcutt, Judy Novak, DonamcLachlan, Network Intrusion Detection & Analysis's Handbook, 2nd Ed, New Ride, September, 2000.

[2] Massimo Bernaschi, Emanuele Gabrielli and Luigi V. Mancini, "Operating System Enhancements to Prevent the Misuse of System Calls", CCS'00 of ACM, pp.174-183, 2000.

[3] Denning, Dorothy E., "An Intrusion Detection Model," IEEE Transactions on Software Engineering, Vol. SE-13, No.2, pp.222-232, 1987.

[4] Bill Hancock, "Security Views," ACM Computers & Security, Vol. 19, No. 7, pp.570-584, 2000.

[5] R. Guski, J. C. Dayka, "Security on z/OS: Comprehensive, current, and flexible, IBM Systems Journal, Vol. 40, No. 3, pp.696-720, 2001.

[6] Bruce Schneier, "Managed Security Monitoring: Network Security for the 21st Centrury", Computer Security Journal, Vol. 17, No. 2, pp.1-12, 2001.

[7] 고종국, 두소영, 은성경, 김정녀, "안전한 FreeBSD 운영체제를 위한 접근 제어 시스템", 한국정보처리학회 추계 학술발표논문집, 제8권, 제2호, pp-847-850, 2001.