네트워크 침입자탐지기법 분석과 대응★

윤동식*

요 약

Connection hijacking은 TCP 스트림을 자신의 머신을 거치게 리다이렉션 할 수 있는 TCP 프로토콜의 취약성을 이용한 적극적 공격 (Active Attack)이다. 리다이렉션을 통해 침입자는 SKEY와 같은 일회용 패스워드나 Kerberos와 같은 티켓 기반 인증 시스템에 의해 제공되는 보호 메커니즘을 우회할 수 있다. TCP 접속은 누군가 접속로 상에 TCP 패킷 스니퍼나 패킷 생성기를 가지고 있다면 대단히 취약하다. 스니퍼의 공격으로부터 방어하기 위하여 일회용 패스워드나 토큰 기반 인증과 같은 사용자 식별 스킴이 사용되어지고 있다. 이들은 안전하지 않은 네트워크상에서 스니핑으로부터 패스워드를 보호하지만 이러한 방법들은 데이터 스트림을 암호화하거나 사인하지 않는 한 적극적인 공격으로부터 여전히 취약하다. 많은 사람들이 적극적 공격은 대단히 어렵고 그만큼 위협도 적을 것이라고 생각하고 있지만 여기서는 이러한 환상을 깰 수 있도록 유닉스 호스트에 성공적으로 침입한 대단히 적극적 공격을 제시한다. 최근 이론적으로 알려진 이 취약점을 공격할 수 있는 도구가 인터넷 상에 공개되어 이에 대한 대책이 요구되고 있다. 본 논문에서는 무선네트워크 상에서 침입자탐지 분석기법에 대하여 제안한다.

Analysis & defence of detection technology in network Attacker

Yun Dong Sic*

ABSTRACT

Connection hijacking attack using the vulnerability of the TCP protocol to redirect TCP stream goes through your machine actively (Active Attack). The SKEY such as one-time password protection mechanisms that are provided by a ticket-based authentication system such as Kerberos or redirection, the attacker can bypass.Someone TCP connection if you have access on TCP packet sniffer or packet generator is very vulnerable. Sniffer to defend against attacks such as one-time passwords and token-based authentication and user identification scheme has been used. Active protection, but these methods does not sign or encrypt the data stream from sniffing passwords over insecure networks, they are still vulnerable from attacks. For many people, an active attack is very difficult and so I think the threat is low, but here to help break the illusion successful intrusion on the UNIX host, a very aggressive attack is presented. The tools available on the Internet that attempt to exploit this vulnerability, known as the recent theoretical measures is required. In this paper, we propose analysis techniques on a wireless network intruder detection

Key words : Analysis & defence of detection technology

접수일(2013년 5월 6일), 수정일(1차: 2013년 5월 15일), 게재확정일(2013년 5월 16일)

* 안동과학대학교 의무부사관과

1. 서 론

오늘날 네트워크에 대한 의존도와 규모가 커지고, 통신선로의 고속화 및 대량화가 이뤄짐에 따라 네트워크 상에서 발생되는 트래픽의 양은 더욱더 증가하게 되었고, 이로 인한 병목현상과 시스템 장애 등으로 인해 응답 속도의 저하뿐만 아니라 네트워크 전체의 다운 현상까지도 초래하고 있다. 이러한 상황은 네트워크 관리에 대한 요구를 증대시키고 있다.[1][2][3].

TCP/IP 기반의 인터넷 관리는 표준 프로토콜인 SNMP를 이용하며, 각 관리 대상 정보를 객체화(Object)하여 집합으로 표현한 관리 정보 데이터베이스(MIB)를 기본으로 관리를 수행한다[3][4]. SNMP의 중앙 집중 관리 구조에서 벗어나 분산 관리 형태의 개념을 채택한 RMON은 원격 세그먼트의 효과적이고 효율적인 관리를 위해 요즘 많은 관심을 불러일으키고 있으나, RMON probe를 탑재한 고가의 라우터나 허브 장비를 갖추고 있어야 하므로, 이 또한 네트워크 관리비용에 대한 큰 부담을 안게 된다.

Connection hijacking은 TCP 스트림을 자신의 머신을 거치게 리다이렉션 할 수 있는 TCP 프로토콜의 취약성을 이용한 적극적 공격 (Active Attack)이다. 리다이렉션을 통해 침입자는 SKEY와 같은 일회용 패스워드나 Kerberos와 같은 티켓 기반 인증 시스템에 의해 제공되는 보호 메커니즘을 우회할 수 있다. TCP 접속은 누군가 접속로 상에 TCP 패킷 스니퍼나 패킷 생성기를 가지고 있다면 대단히 취약하다.

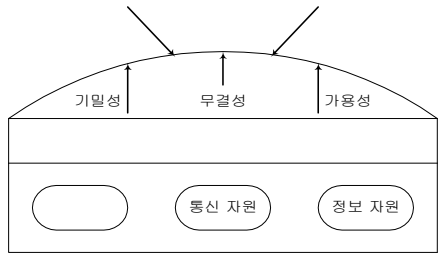
현재 TCP/IP 환경의 네트워크 관리 구조는 표준 프로토콜인 SNMP를 이용하여 네트워크 상의 장비들을 폴링함으로써 관리 정보인 MIB을 이용하여 분석하는 형태로 이뤄지고 있다. 그러나 이 SNMP의 표준 MIB인 MIB-II는 SNMP 에이전트가 탑재된 시스템 자신만의 데이터를 보유하고 있기 때문에 LAN과 같은 많은 시스템들이 복잡하게 존재하는 네트워크 상에서의 전체 트래픽에 대한 통계 자료 또는 호스트들 간의 트래픽 발생 현황 등을 얻어내기가 어렵다[5][6].

또한 대규모 네트워크에서 관리 시스템이 관리 대상 장비와의 정보 교환을 위해 주기적으로 폴링을 수행하게 되면, 이로 인해 발생되는 관리 트래픽은 오히려 네트워크 부하를 높이는 장애요인이 될 수 있다. 이러한 문제점의 대안으로서 RMON이 등장하게 되었으며, 각 세그먼트 마다 트래픽 모니터링을 수행하는 RMON 장비를 두고, 관리 시스템은 RMON 장비로부터 가져온 세그먼트 전체 데이터를 토대로 네트워크 관리를 수행하게 된다[7].

2. 침입자탐지제어 시스템 자원

어떤 사람에게 시스템 자원의 사용허가를 결정하는데 있어서 논리적 접근통제는 요청된 접근 유형에 대하여 인가된 사용자인지의 여부를 조사한다. 이 조사는 사용자가 시스템 전체를 사용하는 것이 인가되었는지 여부를 묻는 질문과는 다르다.

(그림 1)에서 시스템은 접근요청 인정을 결정하기 위해 다양한 기준을 사용한다. 일반적으로 다양한 기준들이 서로 조합되어 사용된다. 침입자탐지제어의 구현과 운영에 관련된 많은 장점과 복잡성은 지원되는 다양한 종류의 사용자 접근과 연관되어 있다.



(그림 1) 접근 통제 목적

접근 요청을 인정하기 위하여 4 가지 단계가 필요하다. 제 1단계는 신분으로서, 침입자탐지제어의 대부분은 보통 식별 및 인증을 통해 얻어지는 사용자의 신분에 기반을 두고 있다. 책임추정을 지원하기 위해 신분은 보통 유일해야 하지만 그룹 식별 또는 무명인이 될 수 있다. 예를 들어, 공공정보 분배시스템에서 연구자 개인들은 알려지지 않은 채 “연구원”이라 불리는 큰 그룹으로 식별 및 인증이 제공될 수도 있다.

제 2단계는 역할이다. 정보에 대한 접근은 할당된 업무나 접근을 원하는 사용자의 기능 즉, 역할에 의해 통제된다. 접근권한은 역할 명에 따라 분류되고, 자원

의 사용은 연관된 역할을 수행하도록 허가된 개인으로 제한된다. 역할의 사용은 침입자탐지제어를 제공하는 매우 효과적인 방법이 될 수 있다. 역할을 정의하는 과정은 조직의 운영에 대한 철저한 분석에 기반을 두어야 하고, 조직 내의 광범위한 사용자로부터의 입력을 포함하여야 한다.

제 3단계로서 위치는 특별한 시스템 자원에 대한 접근은 물리적이거나 논리적인 위치에 기반을 둘 수 있다. 조직 내부 사이트의 사용자가 외부 사이트의 사용자 보다 많은 접근권한을 가지는 것처럼 네트워크 주소를 기반으로 사용자를 제한할 수 있다.

제 4단계는 시간이다. 시간 또는 요일 등에 기반을 둔 접근제한은 많이 사용된다. 예를 들어, 개인의 비밀 파일 사용은 오직 일상 근무 시간에만 허용하고 오전 8시 이전과 오후 6시 이후, 주말과 공휴일에는 거부하는 것이다.

시스템에 접근하기 위해서는 3 가지 시스템 자원이 필요하다. 첫 번째가 트랜잭션인데 일부 일상적 트랜잭션은 직접 실행될 수도 있지만, 더 복잡한 것은 사람의 개입을 필요로 한다. 이와 같은 경우에 계정 번호를 이미 알고 있는 컴퓨터는 트랜잭션이 발생하는 기간동안에 특정 계정을 부여받은 직원의 접근을 허용할 수 있다. 트랜잭션이 완료되면 접근 허가는 종료된다. 이것은 사용자에게 접근할 수 있는 계정에 대한 선택의 여지를 주지 않으며, 따라서 잘못될 가능성을 줄일 수 있다. 또한 직원들이 잘 알려진 사람이나 이웃의 계정을 검색하지 못하게 하여 프라이버시를 강화할 수도 있다.

두 번째는 서비스 제한이다. 서비스 제한은 응용프로그램을 이용하는 동안 발생하거나, 자원의 소유자나 경영자에 의해 미리 설정된 변수에 의존하는 제한을 말한다. 예를 들어, 어느 특별한 소프트웨어 패키지가 회사에서 다섯 명의 사용자에 대해서만 동시에 사용할 수 있도록 허가된 경우에는 응용 프로그램을 사용할 수 있는 허가를 받은 사용자일지라도 여섯 번째 사용자의 접근은 거부될 것이다. 다른 종류의 서비스 제한은 응용 프로그램의 내용 또는 산술적인 경계치에 기반을 두고 있다. 예를 들어, ATM 기계는 일정 금액 한도 이상에 대한 계좌간의 이체를 제한하거나 ATM에서 인출할 수 있는 하루의 최대 금액을 300만원으로 제한할 수 있다.

마지막 세번째가 공통 접근 모드이며, 언제 접근을 허용할 것인가에 대한 기준이외에도 접근의 종류나 접근 모드를 고려하는 것이다. 접근 모드의 개념은 침입자탐지제어의 기본 요소이다.

응용 프로그램에서 더 자주 발견되는 특별한 접근 모드는 첫째가 생성 권한으로서 사용자가 새로운 파일, 기록, 필드를 생성하는 것을 허용한다는 것이고, 둘째는 찾기 권한으로서 사용자가 디렉토리 내에 있는 파일들의 목록을 작성하는 것을 허용한다는 것이다. 물론, 이들 기준은 서로 결합해서 사용될 수 있다.

3. 침입자탐지제어 방법

본 논문에서는 침입자탐지제어의 주체와 객체에 대해 접근을 수행함에 있어 매트릭스 방법을 제안한다. 그리고 제안된 매트릭스 방법이 각각의 환경에서 어떻게 적용되는지 나타낸다. 또한 어떤 하드웨어적 구성요소들이 필요한가를 나타내는데, 메모리, 보조 기억장치의 파일 혹은 데이터, 파일 디렉토리, 하드웨어 장치, 데이터 구조, 운영체제의 테이블, 특수 권한의 명령어, 패스워드 및 사용자 인증 메커니즘, 보호 메커니즘등과 같은 유형의 자원들은 접근 통제의 대상으로서 운영체제에 의한 보호가 필요한 자원들이다.

시스템 자원에 대한 접근은 자원의 공유를 위해서 수행되는 필연적인 활동이며, 이를 올바로 통제하는 것이 정보보호를 위한 중요한 시작이 된다. 따라서 본 논문에서는 이러한 접근에 관여하는 개체들의 행위 여부에 따라 개체들을 주체와 객체로 구분하여 침입자탐지제어 방법을 제시하고자 한다.

우선, 주체와 객체는 접근을 수행하는데 있어 어떤 개체의 행위가 능동적인지, 수동적인지를 구별하기 위해서 사용된다. 주체는 사용자나 프로세스와 같이 능동적인 개체를 의미하며, 객체는 파일, 메모리, 프린터 등의 자원과 같이 수동적인 개체를 의미한다. 그러나 이러한 구분은 상황에 따라 달라질 수 있다. 이러한 주체와 객체의 관계를 이용하여 접근 통제를 구현하는 메커니즘에는 접근 통제 매트릭스(ACM : Access Control Matrix), 접근 통제 목록(ACL : Access

Control List), 권한(capability)등이 있다.

접근 통제 매트릭스는 주체와 객체간에 허용된 접근 모드에서 주체를 행으로, 객체를 열로 하여 테이블로 나타낸 것이다. 이때 접근 통제 매트릭스의 각 요소들은 주체가 객체에게 행할 수 있는 접근 방식을 명시한다. 접근 통제 매트릭스의 예로는 <표 1>에서와 같이 UNIX에서 사용자와 파일간의 허용접근 모드를 테이블로 나타낸다. <표 1>에서 사용자 user_1은 file_1에 대해서는 아무런 접근 권한도 없으나, file_2에 대해서는 실행 권한을, file_3에 대해서는 실행과 읽기 권한을 갖고있음을 알 수 있다.

<표 1> 접근 통제 매트릭스

	file_1	file_2	file_3
user_1	-	execute	execute, read
user_2	read, write	execute	execute, read, append, write

이때, 주체의 관점에서 접근 통제 매트릭스를 해석한 것이 권한이다. 권한은 주체의 접근 권한을 의미하며, 이는 접근 통제 매트릭스의 행에 해당한다. 한 주체가 어떤 새로운 객체를 생성했을 때, 그 주체는 다른 주체들에게 자신이 생성한 객체에 대한 접근 권한을 부여할 수 있다. 권한을 소유한 주체는 명시된 접근 모드에 따라 객체에 접근할 수 있다. 시스템은 시스템의 최상위 수준에게 각 사용자의 권한 목록을 관리한다. 사용자들은 자신이 새로운 객체를 만들지 않는 이상 이 목록에 권한을 추가할 수 없다. 하지만 사용자들은 자신의 객체에 대해서는 접근 권한을 다른 사용자에게 부여할 수 있고, 이미 주어진 접근 권한을 취소할 수도 있다. 이것은 어떤 객체에 누가 접근했는지에 대한 전반적인 관리가 어렵다는 것과 권한의 취소가 어렵다는 보안 관리상의 복잡함 때문에 보안 메커니즘으로 사용되지 않는다.

접근 통제의 목적은 객체에 대한 주체의 접근을 제한하는 것뿐만 아니라 '주체가 객체에 무엇을 하는 것'을 제한하는 것이다. 절차지향 접근 통제에서는 객체에 대한 접근을 통제하는 절차가 존재한다. 이러한 절차는 특정한 유형의 접근만을 허용하는 객체를 둘러싸고 있는 캡슐을 형성한다. 따라서 절차는 신뢰할 수 있는 인터페이스를 통하여 수행되는 객체에 대한 접근을 요청할 수 있다.

절차지향 접근 통제는 정보 은닉의 원리를 구현한다. 즉, 객체의 구현 수단은 객체에 대한 통제 절차에게만 알려진다. 그러나 절차지향 접근 통제는 효율성에서 적지 않은 문제를 수반할 수 있다.

네트워크상의 침입자탐지제어에는 네트워크 접근 실체, OSI 계층 보안 서비스, OSI 계층 침입자탐지제어가 있다. 네트워크 접근 실체에는 Physical Entities (Real Open Systems), Logical Entities (OSI Layer Entities, Files, Organizations), Human Users, Active Entity (Initiator, Subject), Passive Entity (Target, Object)가 있으며, OSI 계층 보안 서비스는 <표 2>와 같다.

OSI 계층 접근 통제는 네트워크를 연결하는 도중이나 연결을 통한 데이터의 전송중 침입자탐지제어를 말하며 네트워크 계층, 트랜스포트 계층, 응용 계층이 있다.

<표 2> OSI 계층 보안 서비스

보 안 서 비 스	1	2	3	4	5	6	7
Peer entity authentication			○	○			○
Data origin authentication			○	○			○
Access control service			○	○			○
connection confidentiality	○	○	○	○			○
connectionless confidentiality		○	○	○			○
Selective field confidentiality							○
Traffic flow confidentiality	○		○				○
connection integrity with recovery				○			○
Connection integrity without recovery			○	○			○
Selective field connection integrity							○
Connectionless integrity			○	○			○
Selective field connectionless integrity							○
Non-repudiation with proof of origin							○
Non-repudiation with proof of delivery							○

4. 메커니즘의 기술적 구현

대부분의 메커니즘이 내·외부의 침입자탐지제어를 제공하기 위해 개발되어 왔으며 정밀도, 복잡도, 비용 측면에서 상당히 다양하다. 이러한 방법은 상호 배타적이지 않으며 흔히 서로 조합되어 사용된다. 관리자는 가장 적합하고, 비용적으로 효과적인 논리적 접근 통제를 선택하기 위해 소속된 조직의 보안 요구사항을 분석할 필요가 있다.

4.1 내부의 침입자탐지제어

내부의 침입자탐지제어는 사용자나 사용자 그룹이 시스템 자원을 가지고 할 수 있는 일과, 할 수 없는 일들을 분리하는 논리적인 수단이다. 내부적인 접근 통제 방법에는 패스워드, 암호, 접근 통제 목록, 제한된 사용자 인터페이스, 레이블 등, 다섯 가지가 있다.

패스워드는 대개 사용자 인증과 관련이 있다. 또한 패스워드는 PC를 포함한 많은 시스템의 데이터와 응용 프로그램을 보호하는데 쓰이기도 한다. 패스워드 기반의 침입자탐지제어는 매우 다양한 응용 프로그램에 이미 포함되어 있기 때문에 비용이 많이 들지 않는다. 그러나 사용자가 부가적인 응용 패스워드들을 기억하는 것이 어려우므로 적어 놓거나 추측하기 쉬운 패스워드를 선택할 경우 침해사고로 연결될 수 있다. PC 응용 프로그램을 위한 패스워드 기반의 접근 통제는 사용자가 운영체제에 접근할 수 있다면 쉽게 우회할 수 있다.

논리적 침입자탐지제어에 쓰일 수 있는 또 다른 메커니즘은 암호화다. 암호화된 정보는 오직 적합한 암호키를 가진 사람에 의해서만 복호화될 수 있다. 이것은 랩탑 컴퓨터나 플로피 디스켓과 같이 강한 물리적 침입자탐지제어가 제공될 수 없는 경우에 특히 유용하다. 따라서 정보가 랩탑 컴퓨터에 암호화되어 있으면 랩탑이 도난을 당하여도 정보에는 접근할 수 없다. 암호화가 강한 침입자탐지제어를 제공할 수 있는 반면에 강력한 키 관리가 필요하다. 암호의 사용은 가용성에도 영향을 미칠 수 있다. 예를 들어 키를 분실하거나 도난을 당한 경우 또는 읽기와 쓰기 오류가 발생하는 경우 정보를 복호화할 수 없다.

침입자탐지제어목록이란 특정 시스템 자원의 사용을 허가 받은 사용자(그룹, 장비, 프로세스를 포함)와 그들이 허가 받은 접근의 종류에 대한 등록을 말하며 접근목록은 기능과 유연성에 따라 상당히 다르다. 일부는 소유자, 그룹, 그리고 사용자 등 미리 결정된 그룹에 대한 규정만을 허용하는 반면에 진보된 침입자탐지제어목록은 사용자가 정의한 그룹과 같이 좀더 많은 융통성을 제공한다. 또한 더욱 진보된 침입자탐지제어 목록은 특정한 개인이나 그룹에 대한 접근을 명백히 거부하는데 사용될 수 있다. 더욱 진보된 침입자탐지제어목록인 경우 통제가 기술적으로 어떻게 구현될 것인가에 따라 접근은 정책 수립자의 재량에 따르거나 사용자 개인에 의해 결정될 수 있다. 기본적인 침입자탐지제어목록은 대체로 소유자, 그룹, 그리고 모든 사용자의 개념에 기반을 둔다. 각각에 대해서 자원의 소유자 특정 접근 모드를 설정한다. 소유자는 보통 자원을 생성한 사람이지만 어떤 경우에는 생성한 사람의 신분을 무시하고 자원의 소유권이 자동적으로 프로젝트 관리자로 지정될 수도 있다. 그리고 소유자에게 지정된 권한 이외에 각 자원들은 사용자의 그룹과 관련이 있다. <표 3>에서 그룹의 회원인 사용자는 비회원과 상이한 접근모드를 허가 받는다. 사용자 그룹은 부서, 프로젝트, 또는 특별한 조직에 알맞게 다양한 방식에 의해서 배정된다.

진보된 침입자탐지제어목록은 정보를 복잡하게 공유하는 경우에 매우 유용하다. 개별 시스템 정책을 구현하는데 많은 융통성을 제공하고, 관리자의 보안 요구사항에 부합하도록 만들 수 있다. 서로 상충하는 침입자탐지제어목록의 경우 접근을 결정하는 규칙들이 모든 구현에 따라 서로 일치하지 않아 보안관리자를 혼란시킬 수 있다. 따라서 이러한 시스템을 도입할 경우에는 관리자가 이를 정확히 사용하여야 한다.

<표 3> 급여파일에 대한 침입자탐지제어목록의 예

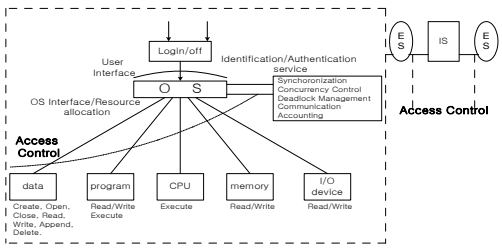
급여파일에 대한 진보된 침입자탐지제어목록의 예:	
급여관리자 :	R, W, E, D
홍 길 동 :	R, W, E, -
이 순 신 :	-, -, -, -
강 감 찬 :	R, W, E, -
김 유 신 :	R, W, E, -
유 관 순 :	R, -, -, -
급여사무실 :	R, -, -, -
모든사용자 :	-, -, -, -

침입자탐지제어목록과 함께 흔히 사용되는 것이 제

한된 사용자 인터페이스이다. 제한된 사용자 인터페이스는 특정 기능이나 자원에 대한 접근권한이 없는 경우에는 접근 요청을 하지 못하도록 한다. 메뉴, 데이터 베이스 뷰, 물리적으로 제한된 사용자 인터페이스 등의 세 가지 종류가 있다. 사용자는 대체로 메뉴 형식으로 제공되는 명령어만을 실행할 수 있다.

사용자를 제한하는 또 다른 방법은 사용자가 실행할 수 있는 시스템 명령어를 제한하는 쉘(shell)을 이용하는 것이다. 메뉴와 쉘의 사용은 흔히 시스템을 사용하기 쉽게 만들 수 있고, 오류를 감소시키는 데 도움을 줄 수 있다. 데이터베이스 뷰는 데이터베이스 안에 있는 데이터에 대한 사용자 접근을 제한하기 위한 메커니즘이다. 사용자는 데이터베이스에 접근을 요구하지만 그 사용자가 데이터베이스 내의 모든 데이터에 대한 접근을 가질 필요는 없다. 뷰는 필드의 내용에 따른 접근 요구사항과 같은 복잡한 접근 요구사항을 제공하는데 사용될 수 있다. 물리적으로 제한된 사용자 인터페이스 또한 사용자의 기능을 제한한다.

마지막으로 보안 레이블(label)은 침입자탐지제어, 보호수단 규정, 또는 부가적인 지시사항 등 다양한 목적을 위해 사용될 수 있다. 많은 구현에 있어서 일단 레이블이 정해지면 이는 변경될 수 없다. 침입자탐지제어에서 레이블은 사용자 세션에 할당된다. 사용자는 특정 레이블을 가진 세션만을 시작할 수 있다. 예를 들어, “조직 소유 정보”라는 레이블이 붙은 파일은 이에 대응하는 레이블을 가진 사용자 세션을 제외하고는 읽거나 접근할 수 없다. 오직 제한된 사용자 집단만이 그와 같은 세션을 초기화 할 수 있다. 세션의 레이블과 접근하고자 하는 파일의 레이블은 세션의 출력을 레이블 하는데 사용될 수 있어, 정보가 시스템 상에서 처리되는 동안 일정하게 보호되도록 보장한다.



(그림 2) 침입자탐지제어 시스템 환경

레이블 사용에 있어서 관리와 비 융통성이 상당한 장애가 될 수 있음에도 불구하고 레이블은 침입자탐지제어를 견실하고 균일하게 적용된다. (그림 2)는 침입자탐지제어 시스템 환경을 나타낸다.

4.2 외부의 침입자탐지제어 관리

외부의 침입자탐지제어는 내부 시스템과 외부의 사람이나 시스템과의 상호 작용을 통제하는 수단이다. 외부의 침입자탐지제어는 보호되고 있는 시스템과 네트워크 사이에 분리된 물리적 장치의 사용을 포함하는 광범위하고 다양한 방법이 사용된다. 이들 가운데 포트 보호장비(PPD)는 컴퓨터 자체의 침입자탐지제어 기능에 앞서 독립적으로 포트에 대한 접근을 인가한다.

흔히 침입차단시스템이라 불리는 안전한 게이트웨이는 두 개의 망 즉, 사설망과 악의적인 해커를 끌어들이는 인터넷과 같은 공중망 사이에서 접근을 차단하거나 필터링하는 기능을 수행한다. 안전한 게이트웨이는 내부 사용자가 외부망과 연결하는 것을 허용하고 동시에 악의적인 해커가 내부 시스템을 손상시키는 것을 방지한다. 마지막으로 호스트 기반 인증은 요청을 하는 사용자의 신분 대신에 접근 요청에 사용되는 호스트에 기반을 둔 방법이다. 오늘날 사용되는 많은 망 응용 프로그램은 접근 허용여부를 결정하기 위하여 호스트 기반 인증을 사용한다. 어떤 환경에서는 위장 호스트가 합법적인 호스트와 물리적으로 가까운 위치에 있을 경우 합법적인 호스트로 흉내내기가 용이하다. 일부 호스트 기반 인증 시스템의 오용을 방지하기 위한 보안 수단을 이용할 수 있다.

4.3 침입자탐지제어 관리

침입자탐지제어의 가장 복잡하고 어려운 점은 시스템 상의 사용자 접근을 구현하고, 감시하고, 변경하고, 검사하며 그리고 권한을 제거하는 것이다. 이러한 것들은 각 사용자의 접근 종류에 관한 실제적인 결정을 포함하지 않지만 많은 노력을 요구하는 업무일 수 있다. 접근에 대한 결정은 조직의 정책, 직원의 업무와 업무 기술서, 정보의 중요도, 사용자가 알아야할 사항 그리고 다른 많은 요인에 의해 결정될 수 있다. 침입

자탐지제어 관리에는 중앙화, 분산화 또는 이들의 조합 등 세 가지의 방법이 사용된다. 각각은 상대적인 장·단점을 가지고 있으며 어느 것이 주어진 상황에 가장 적합한가는 조직의 특성과 환경에 따라 다르다.

중앙관리 방식은 한 사무실이나 개인이 침입자탐지제어 구성에 대한 책임을 갖는다. 사용자의 정보 처리가 변경될 필요가 있을 경우 오직 중앙 사무실을 통해서만 변경될 수 있으며 적합한 관리자에 의해서 요청이 승인된 후 변경된다. 침입자탐지제어 권한이 매우 적은 수의 사람에게만 주어지기 때문에 정보에 대한 엄격한 통제가 가능하다. 각 사용자의 계정은 중앙에서 감시 될 수 있고 조직을 떠나는 사용자의 모든 접근을 쉽게 종료시킬 수 있다. 상대적으로 소수의 사람만이 프로세스를 감시하므로 철저하고 일률적인 절차와 기준을 어렵지 않게 집행할 수 있다. 그러나 빠른 변경이 필요할 때는 중앙 관리 사무실을 거치는 것이 방해가 되거나 많은 시간이 소요될 수 있다.

분산관리의 경우 접근은 파일의 소유자나 생성자 그리고 흔히 기능 관리자에 의해 직접 통제된다. 이것은 통제 대상에 대해 가장 많은 책임을 갖고 있거나 정보와 정보의 사용에 가장 익숙하고 누구에게 어떤 종류의 접근이 필요한지를 가장 잘 판단할 수 있는 사람에 의해 유지되는 것이다. 그러나 분산관리는 사용자 접근과 권한을 인가하기 위한 절차와 기준에 대하여 소유자 및 생성자들 사이의 일관성을 유지하기가 어려울 수도 있다. 또한 요청이 중앙에서 처리되지 않을 경우 주어진 시간에 시스템 상의 모든 사용자 접근을 관찰하는 것이 더 어려울 수 있다.

혼합 방법은 중앙화와 분산 관리를 조합한 것이다. 중앙 관리는 가장 넓고 기본적인 접근에 책임을 지고 파일의 소유자 및 생성자는 자신들의 통제하에서 접근의 종류 또는 파일에 대한 사용자의 기능 변경을 통제하는 것이 전형적인 배열이다. 혼합 방법의 주된 단점은 어떠한 접근이 지역적으로 설정 가능한가와 어느 것이 중앙에서 설정 가능한가를 알맞게 정의하는 것이다.

4.4 침입자탐지제어 알고리즘

침입자탐지제어를 위하여 필요한 action에 연결될 Initiator/Operation/Operand-bound ACI 생성알고리즘 및 Bound ACI 검증 및 ADI 유도 알고리즘, 침입자탐지제어 배경정보 획득 알고리즘, 접근결정 알고리즘을 제시한다.

(1) Action-bound ACI 생성 알고리즘

Generate action-bound ACI /* 침입자탐지제어를 위하여 필요한 action에 initiator/operation/operand-bound ACI를 연결 */

Inputs

- Initiator-bound ACI
- Operation-bound ACI
- Operand-bound ACI
- target identity
- action or action reference
- validity period
- interaction policy identifier

Outputs

- status
- action-bound ACI
- security token
- retained ADI reference

(2) Bound ACI 검증 및 ADI 유도 알고리즘

Verify bound ACI and derive ADI

Inputs

- bound ACI(Initiator, target, action, operation or operand)
- security token
- reference to action
- validity period
- interaction policy identifier

Outputs

- status
- action or action reference
- ADI

(3) 침입자탐지제어 배경정보 획득 알고리즘

Get contextual information /* 침입자탐지제어

결정을 위하여 요구되는 배경정보를 획득 */

Inputs
- reference to action
- context information identifier
- interaction policy identifier

Outputs

- status
- contextual information

(4) 접근결정 알고리즘

Decide access /* 접근이 허용되는지 결정 */

Inputs

- action
- Initiator ADI
- action ADI
- target ADI
- contextual information
- retained ADI reference
- interaction policy identifier

Outputs
- access control decision
- validity period of decision
- identifier of sequence of actions authorized
- retained ADI reference

5. 공격탐지 및 방지대책

hijacking 공격에 대한 탐지 방법이은 다음과 같다.

○ desynchronized 상태 탐지

○ 접속 양단의 일련번호를 비교함으로써 사용자는 이 접속이 desynchronized 상태인지를 탐지할 수 있다. 이 방법은 TCP 스트림을 통해 전송되는 일련번호가 공격자에 의해 변경되지 않았다고 가정할 경우에 가능하다.

○ Ack storm 탐지

○ 지역 이더넷 상의 TCP 트래픽에 대한 통계자료는 공격이 없는 일반적인 상황에서는 전체 telnet 패킷 당 데이터 없는 ACK 패킷의 비율이 대략 45% 정도이다. 이는 telnet 세션은 대화형 세션으로 사용자에 의해 타이프된 모든 문자는 에코되어지고 확인되어 진다는 것을 알 수 있다. 공격이 수행될 경우 이러한 통계값들이 변하게 될 것이다.

○ 특정 세션에서 패킷 유실 및 재전송 증가 탐지

○ 공격 중에는 비정상적으로 높은 비율의 패킷 유실 및 재전송이 발생하므로 공격임을 알 수 있다. 이는 사용자에 대한 응답시간의 지연을 의미한다. 패킷 유실 증가는 다음의 이유에 의해 발생한다.

○ ACK storm에 기인한 네트워크의 특별한 부하

○ 공격자의 스니퍼에 의한 패킷 상실. 이러한 패킷 상실은 네트워크 부하를 증가시키는 경향이 있음

○ 기대치 않은 접속 리셋

○ 사용자는 공격 프로토콜이 적절히 수행되지 않을 경우에 접속 초기 상태에서 세션의 접속 리셋을 경험할 수 있다. 공격의 약 10%가 성공하지 못하며 이에 따라 접속 종료(사용자에게 매우 가시적으로 나타남)나 non-desynchronized 접속(공격자는 스트림을 리다이렉트할 수 없음)으로 끝난다.

응용세션에서의 이러한 공격으로부터의 방어는 암호화된 커버로스 스킴(응용계층)이나 TCP 암호화 구현(TCP 계층)이다. 데이터 흐름의 암호화는 내용에 대한 침범이나 변조를 방지한다. 데이터에 대한 서명도 사용되어 질수 있다. PGP는 안전한 전자우편 전송의 한 예이다.

6. 결 론

Connection hijacking은 TCP 스트림을 자신의 머신을 거치게 리다이렉션 할 수 있는 TCP 프로토콜의 취약성을 이용한 적극적 공격 (Active Attack)이다. 리다이렉션을 통해 침입자는 SKEY와 같은 일회용 패스워드나 Kerberos와 같은 티켓 기반 인증 시스템에 의해 제공되는 보호 메커니즘을 우회할 수 있다. TCP 접속은 누군가 접속로 상에 TCP 패킷 스니퍼나 패킷 생성기를 가지고 있다면 대단히 취약하다.

침입자탐지제어의 구현과 운영에 관련된 많은 장점과 복잡성은 다양한 종류의 사용자 접근과 연관되어

있다. 접근 요청을 인정하기 위해서는 신분, 역할, 위치, 시간의 4가지 단계가 필요하고, 시스템에 접근하기 위해서는 트랜잭션, 서비스 제한, 공통 접근의 3가지 시스템 자원이 필요하였다.

본 논문에서는 다양한 시스템 자원을 정의하였고 사용자 및 시스템 소프트웨어와 데이터 등이 적재되는 메모리에 대한 여러 가지 보호 방법을 설명하였다. 또한 시스템 자원에 대한 사용자의 접근을 통제하는 접근 통제 메커니즘을 설명하였다. 그리고 메커니즘 구현 예를 제시하였고 침입자탐지제어의 주체와 객체에 대해 접근을 수행하는 매트릭스 방법을 제안하였다. 또한 어떤 구성요소들이 필요한가를 나타냈는데, 본 논문에서 제안한 보안 메커니즘으로 어떤 객체에 누가 접근했는지에 대한 전반적인 관리가 어렵기 때문에 목록을 관리해야만 한다. 기술적 구현은 내부 접근 통제, 패스워드, 암호화, 침입자탐지제어목록으로 나누어지며, 기본적인 침입자탐지제어목록은 대체로 소유자, 그룹, 그리고 모든 사용자의 개념에 기반을 둔다. 각각에 대해서 자원의 소유자가 특정 접근 모드를 설정한다.

소유자는 보통 자원을 생성한 사람이지만 어떤 경우에는 생성한 사람의 신분을 무시하고 자원의 소유권이 자동적으로 프로젝트 관리자로 지정될 수도 있다. 파일 소유자는 흔히 자신의 자원에 대한 모든 권한을 갖는다.

인터넷에서 모든 사람들의 관심이 현재의 IPv4를 대체하고있는 IPv6의 출현에 따라, 공격의 증가와 안전한 시스템의 필요성은 인터넷 사외를 위한 안전한 전송계층의 개발 및 사용을 요구하고 있다. 프라이버시를 보호하기 위해서 사인을 하고 결국 암호화된 데이터의 전송이 선택적으로 가능해야 한다. 데이터에 대한 서명은 현재의 TCP 체크섬이 신뢰성 있는 서명으로의 대체를 의미한다.

일반적으로 이더넷의 스니핑을 방지하기 위하여 s/key나 커버로스를 사용하는 것만으로 충분하다는 생각은 대단히 위험하다는 것을 깨달아야 한다.

참고문헌

[1] William Stallings, "SNMP, SNMPv2, and RMON : Practical Network Management", Addison-Wesley Publishing Company, 2004

[2] Heng Pan, "SNMP-Based ATM Network Management", Artech House, Inc., 2008

[3] J. Case, M. Fedor, M. Schoffstall, J. Davin, "Simple Network Management (SNMP)", RFC 1157, May 1990

[4] K. McCloghrie, M. Rose, "Management Information Base for Network Management of TCP/IP-based Internets : MIB-II", RFC1213, March 1999

[5] Gilbert Held, "LAN Management with SNMP and RMON" John Wiley& Sons, New York, NY,1996. ISBN 0-471-14736-2

[6] Nathan J. Muller, "SNMP's Remote Monitroing MIB", International Journal of Network Management

[7] Gilbert Held, "LAN Management with SNMP and RMON", John Wiley & Sons, Inc.

[8] http://msdn.miscrosoft.com/library/wcedoc/wceddk

[9] Snajay Dhawan, "Networking DEVICE DRIVERS", VNR Communications Library,

[저자소개]

윤 동 식 (Yun Dong sic)

1992년 관동대학교 정보처리학과 (공학사)
1994년 관동대학교 전자계산공학과 (공학석사)
2000년 관동대학교 전자계산공학부 (공학박사)
1999년~2008년 안동과학대학교 사이버테러대응과 교수
2008년~현제 안동과학대학교 의무부사관과 교수

e-mail : yundos@asc.ac.kr