일괄 보안정책 관리 시스템의 설계 및 구현

김이곤° 신영선 유성훈 안소진 박진섭
대전대학교
gon202@dju.ac.kr°, ysshin@zeus.dju.ac.kr, claile@nate.com, ansolove@nate.com, jspark@dju.ac.kr

Design and Implementation of Batch Security Policy Management System

Yi Gon Kim°, Young Sun Shin, Sung Hun Yu, So Jin An, Jin Sub Park
Daejon University

요 약

오늘날 빠른 정보화로 인한 역기능의 발생으로 인하여 침입탐지, 침입차단 및 방지 시스템들의 다양한 보안 솔루션을 도입하여 사용하고 있다. 하지만 제로 데이 공격과 같이 빠르게 확산될 경우 보안 장비에 빠르게 정책을 적용해야 하지만 보안 장비마다 각기 다른 접근 및 제어 형식으로 인하여 빠르게 대처하고 있지 못하다. 본 논문에서는 이러한 문제점을 보완하기 위해 한번의 정책 주입으로 대규모 네트워크에 설치되어 있는 보안 장비 및 네트워크 장비에 보안정책을 주입 시킬 수 있는 일괄 보안정책 관리 시스템에 대한 설계 및 구현에 대하여 논하고자 한다.

1. 서 론

오늘날의 컴퓨터 네트워크 인프라는 빠른 속도로 발전으로 인하여 다양한 네트워크를 기반으로 사회 전반으로 큰 변화를 가져 왔다. 반면 그에 대한 역기능으로 해킹·바이러스·웜 등을 통한 정보 유출 및 정보의 위·변조 등의 피해가 빈번히 발생하고 있다.

이를 위해 침입탐지, 침입차단 및 방지 시스템 등의 다양한 보안 솔루션을 도입하여 사용하고 있으며, 최근에는 보안 솔루션들을 일관성 있게 중앙에서 통합 관리하는 전사적 보안 관리 시스템(EMS)을 통하여 이기종 보안 솔루션들의 이벤트를 분석하고 통합적으로 관리함으로써 보안 솔루션들의 상호 운용성을 높이게 되었다. 그러나 이런 전사적 보안 관리 시스템(EMS)는 로그를 기반으로 하여 관리자에게 경고만을 알려주기 때문에 문제가 빠르게 대응 할 수 없다.

보안 취약점이 발견되었을 때 그 문제의 존재 자체가 널리 공표되기도 전에 해당 취약점을 악용하여 이루어지는 보안 공격을 "제로 데이 공격"이라 한다.

이것은 공격의 신속성을 의미하는 것으로 일반적으로 컴퓨터에서 취약점이 발견되면 제작자나 개발자가 취약점을 보완하는 패치를 배포하고 사용자가 이를 내려받아 대처하는 것이 관례이나, 제로 데이 공격은 대응책이 공표되기도 전에 공격이 이루어지기 때문에 이러한 공격에 대해 빠른 대처가 필요하다.

따라서 보안 솔루션들의 설치/운영만으로 안전을 보장 받을 수 없다. 특히 대규모 네트워크는 다양한 네트워크 장비와 보안 솔루션으로 구성 되어있어 장비들에 대하여 각각의 장비에 맞게 수동적으로 보안 정책을 적용하고 있기 때문에 이러한 수동적인 작업으로는 제로 데이 공격과 같이 빠르게 확산되는 웜 바이러스와, 트래픽에 대한 일괄적인 통제가 어렵고 즉각적인 대응을 수행하지 못하였을 경우 많은 피해가 발생하게 된다.

따라서 대규모 네트워크를 대상으로 발생하는 여러 가지 보안 사고에 대응하기 위해 빠른 정책 설정과 상이한 여러 솔루션들에 대한 공통적인 정책을 적용할 수 있는 기술이 필요하다.

본 논문에서는 이러한 필요성에 의해 대규모 네트워크의 이질적인 네트워크 보안장비에 일괄적인 보안 정책을 적용할 수 있는 일괄보안 정책 관리 시스템에 대하여 설계 및 구현하고자 한다.

2. 관련연구

2.1 취약성의 실태

미국 CERT CC(Computer Emergency Response Team Coordination Center)에 보고된 보안사건 및 바이러스 통계를 보면 1989년 200여건에 불과하였으나, 1995년에는 14,065건, 1998년에는 22,341건으로 매년 증가하고 있다. 국내의 경우에도 해킹 및 일반 Worm, 스팸릴레이 사건이 해매다 증가하고 있다. 또한 인터넷 데이터 분석 협력 협회 분석보고서에 따르면 취약점을 이용한 Worm 바이러스는 전 세계 모든 취약한 서버의 90% 이상을 10분 이내에 감염시킬 수 있어 그 피해가 보다 심각하다고 할 수 있다.

또한 [표 1]에서 보는 봐와 같이 취약점이 발견된 후 취약점을 이용한 웜 발생일이 더욱더 짧아지고 있다. 이러한 취약점을 해결하기 위해서는 본 논문에서 제안하는 일괄 보안관리 시스템을 통해 보안정책을 수립하여 외부로부터 내부의 취약점을 보호할 수 있다.

[표 1] Patch Gap 주기 변화

이름	취약점 발견	웜 발생일
Nimda	2001-09-18	336일
Slammer	2003-01-25	185일
Blster	2003-08-15	26일
Witty	2004-03-20	2일

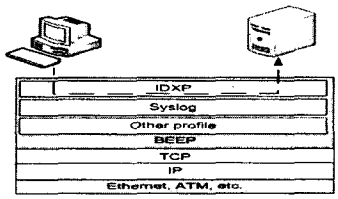
2.2 국·외 기술동향

이기종 보안 시스템 연동을 위한 국제 표준은 표준화 단체인 IETF의 IDWG에서 제안되고 있다. 지금까지는 이기종 보안 시스템간 연동 방안으로서, IDS에서 침입 탐지의 결과를 관리자로 통보하기 위해 IDS 로그 형식 표준안인 IDMEF가 표준안으로 제안되었다. IDMEF에서는 UML의 클래스 다이어그램을 사용하여 로그의 데이터 모델을 정의하였고, 데이터 모델을

실제 표현하는 방법으로 XML을 이용하였다.

IDMEF 기반의 XML 경보 데이터를 관리자로 통보하기 위한 프로토콜로서 IDWG에서는 BEEP기반의 IDXP를 사용하고 있다. BEEP 프로토콜은 IDXP가 TCP/IP 상에서 사용될 수 있도록 해주는 기본 프로토콜이다. BEEP은 TCP 계층에서 동작하는 모든 프로토콜을 블록화하여 프로파일 형태로 제공하며 RFC3080, 3081에 기초하고 있다.

IDXP는 BEEP 상에서 상호 인증, 기밀성 등을 보장하는 프로토콜로서, BEEP 세션 형성 이후에 프로파일 협상 그리고 IDXP 프로파일을 통해서 통신을 수행한다. [그림 1]에서는 BEEP 상에서 IDXP를 이용하여 통신하는 경우를 보여준다.



[그림 1] BEEP 기반 IDXP

2.3 국내 기술동향

2.3.1 ASEN(Adaptive Security for Enterprise Network)

ASEN은 이기종 보안 제품 간의 연동을 위해 어울림정보기술에서 개발한 보안프레임워크이다. 어울림정보기술은 특정 제품들과의 연동을 위한 ASEN API를 제공하므로, ASEN API를 이용하여 특정 제품군과 이기종 보안 제품들은 손쉽게 연동할 수 있다.

ASEN 프레임워크의 설계 목적은 다양한 보안제품으로 구성된 다수의 시스템을 모니터링하고, 상호 유동적으로 결합하여 작동할 수 있는 통신 모델과 제어 모델을 제시함으로써 불필요한 중복작업을 피하고, 보안 위협에 보다 능동적으로 대응할 수 있는 기반을 만드는 것이다. 이를 위해 ASEN은 다음의 사항들에 대해서 정의하고 있다.

○ 상호 통신 방법의 정의, 제품 간 또는 통합관리 서버와의 통신에 있어서 통신방법과 구조를 제안
○ 상호 인증 방법의 정의, 통신에 있어서 신뢰성을 갖기 위한 상호인증 방법을 제시
○ Security Device의 관리정보 표현방법 정의
○ 보안정책 적용, 서로 다른 제품 간의 보안정책을 설정하기 위해 어떠한 방법으로 보안정책을 표현하고 전송하는가에 대하여 제시
○ 통합관리에 필요한 기반 정보를 정의

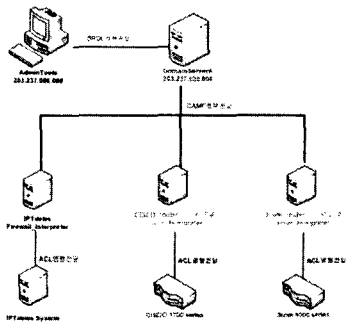
ASEN은 각 보안 제품에 위치한 에이전트와 통합 보안 관리를 위한 관리자 사이에 SNMP형식의 확장된 API 집합을 정의하고 있다. 이러한 ASEN API를 사용함으로써 이기종 보안 제품 간의 연동이 가능하지만, 국내 보안 업계에 아직까지 산업계 보안 표준으로 확립되지 못한 상태이므로 특정 제품에 대해서만이 통합보안관리 할 수 있다.

3. 일괄 보안정책 관리 시스템의 설계

본 논문에서 제안하는 일괄 보안정책 관리시스템은 하나의 네트워크로 구성되어 있는 대규모 네트워크 환경이나 보안관리 시스템이 원거리에 분포되어 있는 경우에 적합한 보안정책 관리기능을 제공한다. 다양한 보안제품으로 구성되는 네트워크는 체계적인 시스템 관리가 가능한 네트워크 환경이어야 한다.

3.1 시스템의 구성

본 논문에서 설계한 일괄 보안정책 관리 시스템은 [그림2]와 같이 관리자가 Admintool을 이용하여 정책을 주입하면 도메인 서버를 거쳐 하부노드에 정책이 주입되게 된다.



[그림 2] 전체 시스템 구성도

3.2 시스템의 주요 기능설계

▶ Admintool 모듈

Admintool은 정책관리 부분, 도메인 서버로 정책을 전달하는 부분, 인증정보를 관리하는 부분, 하위의 구성 정보를 모니터링 하는 부분으로 구성되어 있다.

▶ 도메인 서버

관리자 도구에서 정규화된 형태로 전송된 정책을 하부노드로 전송하는 역할을 담당한다. 여기에서는 도메인서버 등록·해지, 관리자 도구에서 도메인 서버로 정책 전달 등의 기능을 전달한다.

▶ 인터프리터

관리도구에서 작성한 정책을 SPDL(Security Policy Description Language) 형태로 전송하는 것을 도메인 서버에서 각각의 하부노드들에 SPDL형태의 정책을 인터프리터들이 각각의 정보보호제품의 ACL(Access Control List)형태로 변환하는 과정과 정책 적용 여부를 확인 받을 수 있다.

3.3 시스템의 세부 모듈설계

▶ Admintool 모듈

Admintool은 정책관리 부분, 도메인 서버로 정책을 전달하는 부분, 인증정보를 관리하는 부분, 하위의 구성 정보를 모니터링 하는 부분으로 구성되어 있다.

▶ 도메인서버 모듈

도메인서버는 Admintool이나 다른 도메인서버로부터 전송된 정규화된 보안정책을 하부 노드로 전송하는 기능을 수행한다.

▶ 도메인서버 등록

도메인서버는 Admintool과 묶여서 하나의 쌍으로 동작한다. Admintool에서 도메인서버들의 리스트를 요청하면 각각의 도메인서버들은 자신의 이름을 최상위 도메인 서버에게 전달한다. 최상위 도메인 서버가 Admintool에게 하위 도메인서버들의 등록을 위해 등록 요청 메시지를 전달하면 전달받은 메시지를 통해서 등록 선택여부를 결정한다.

▶ 도메인서버 해제

상위, 하위의 계층적인 구조로 이루어진 두 도메인서버 간의 관계를 해제하는 과정으로 도메인 해제를 하게 되면 관리를 받는 도메인서버는 더 이상 상위 도메인서버의 정책을 수용하지 않는다.

▶ 관리도구에서 도메인서버로 정책 전달

관리도구에서 정책을 전달하기 위하여 관리도구가 도메인 서버에게 하위 노드의 정보를 요청하고, 수신된 정보를 바탕으로 정책을 전달하게 된다.

▶ 도메인서버간 정책 전달

등록 과정을 거치고 사전 협상이 완료되면 상위 도메인서버는 자신의 하위 등록된 도메인서버들에게 정책을 전달할 수 있다.

3.4 시스템의 구현

[그림 2]와 같이 환경을 구성 후 Admintool에서 [표 2]와 같이 정책을 삽입하기 위해 작성 후 정책을 적용하면, 도메인 서버에 정책이 전달되어 [표 3]과 같이 DB에 정책이 저장되고 하부장비 인터프리터로 정책이 전달된다. [표 4]에서 보는바와 같이 도메인 서버로부터 받은 정책을 하부장비에 맞게 정책을 ACL로 변환하여 IPTABLE에 정책을 입력하는 내용을 볼 수 있다. 여기에서 보면 상위로부터 전달받은 정책이 라우터의 정책에 맞도록 변환되어 장비에 전달되는 것을 볼 수 있다.

[표 2] Admintool에서의 정책 설정

```
policy DenyTCP110
{
        for( "DomainServerA" )
        {
                incoming
                {
                        if(  src_addr=="203.237.140.41"  and
protocol=="tcp" and dst_port=110 )
                        {
                                deny( 5, essential );
                        }
                }
        }
}
```

[표 3] 도메인 서버에 전달된 주입 정책 로그

```
[root@gons bin]# ./DomainServer 20000
Starting DomainServer at port : 20000
Connection established with remote 203.237.140.190:4098
Receive CommonHeader...
m_MessageType : 1002
m_Option : 1
Receive PolicyHeader...
Recevie SPDL data...
-------------------------------------------------
POLICY     : DenyTCP25
COMMAND    : insert
DOMAIN     : DomainServerA
DIRECTION  : incoming
ACTION     : deny
SRC_ADDR   : 203.237.140.41 ~ 203.237.140.41
SRC_PORT   : -1 ~ -1
DST_ADDR   :
DST_PORT   : 110 ~ 110
PROTOCOL   : tcp
PRIORITY   : 5
-------------------------------------------------
Collision & Adaptation Check...
There is no policy...
New Policy Accepted
////////////////////////////
insert    into    CAMFListData    values(    '','DenyTCP110',
'DomainServerA', '', '-1', '1001', '4005', '2101', '5000', '5', '7002',
'-1', '-1', '3002', '2001', '6000', '203.237.140.41', '203.237.140.41',
'-1', '-1', '', '', '110', '110', '', '')
```

[표 4]는 동일한 정책서버로부터 정책을 수신하여 방화벽 인터프리터에 맞는 형식으로 정책을 변환한 것을 볼 수 있다.

[표 4] IPTABLE에 적용되는 정책(인터프리터)

```
Request hdr len: 12  camf size: 1
spdl recv byte = =288
========RECV CAMF==============
          (3298|3209798304) CAMF ID:-1
          (3298|3209798304) SRC1 ADDR:203.237.140.41
          (3298|3209798304) SRC2 ADDR:203.237.140.41
          (3298|3209798304) DST1 ADDR:
          (3298|3209798304) DST2 ADDR:
          (3298|3209798304) SRC1 PORT:-1
          (3298|3209798304) SRC2 PORT:-1
          (3298|3209798304) DST1 PORT:110
          (3298|3209798304) DST2 PORT:110
==============================
(3298|3209798304) End recv rule...
/sbin/iptables -A INPUT -s 203.237.140.41 -d any -p tcp -m tcp
--dport 110 -j DROP
System : /sbin/iptables -A INPUT -s 203.237.140.41 -d any -p
tcp -m tcp --dport 110 -j DROP
```

4. 결론 및 향후 연구방향

다양한 정보보호제품들은 각기 다른 접근 및 제어 형식을 가지고 있어, 기존의 도입/운영되고 있는 통합 보안 정책 관리 시스템들은 동일 기종에 한해서 일괄 정책 적용이 가능하다. 이로 인해 각기 다른 정보보호제품에 정책을 적용하기 위해서는 각각 정책 설정을 해야 하기 때문에 상당한 시간이 예상된다. 따라서 대규모 네트워크의 보안 사고에 대응하기 위해 각 네트워크 장비에 일괄적인 보안정책을 적용할 수 있는 연구가 필요하다.

본 논문은 기존 네트워크 보안장비의 보안정책 기술 및 동향을 연구하고 대규모 네트워크의 정보보호제품들에 일괄적인 보안정책을 적용할 수 있는 일괄 보안정책 관리 시스템에 대한 설계 및 구현을 하였다.

일괄 보안정책 관리 시스템은 대규모 네트워크의 보안 관리자가 신속하게 보안정책을 적용하고 지능적인 공격 유형에 보다 효율적인 대응을 할 수 있어 기존의 정책설정 방식에 비해 시간이 절약될 뿐 아니라 효율적인 정책 설정을 할 수 있을 것으로 기대된다.

향후 본 논문에서 설계한 일괄 보안정책 관리 시스템에서 정책 전송 시 신뢰관계가 형성될 수 있는 인증 매커니즘에 대한 연구와 정보보호제품들의 ACL로 변환해 주는 인터프리터에 대한 추가적인 연구가 필요하다.

5. 참고문헌

[1] NCSC. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, DEC, 2985

[2]ISO/IEC 9584-8 , Information technology Open Systems Interconnection The Directory : Authentication framework, 1995.

[3] P.Dasgupta, V.Karamcheti, and Z. Kedem, "Efficient and Secure Information Sharing in Distributed, Collaborative Environments", Proceedings of 3rd Internatonal Workshop on Communication based System, April 2000.

[4] 정연서, "대규모 네트워크를 위한 통합 침입탐지 시스템 설계", 한국컴퓨터산업교육학회 논문지, 2002.7.

[5] 신역성, 장종수, "정책기반의 정보보호 시스템 관리기술", 정보보호학회지, 2003.2

[6] 손우용, "통합보안 관리시스템의 침입탐지 및 대응을 위한 보안정책 모델", 컴퓨터정보학회 논문집 제9권2호, 2004.6

[7] 조현정, "차세대 네트워크 보안기술 기반의 침입방지 시스템(IPS)", 한국정보보호과학회, 2005.1

[8] 김용재, "통합 보안정책 관리를 위한 보안정책 기술언어 프로토콜 구현", 대전대학교 석사학위논문 2006.2

[9] 홍철의, "이기종 라우터 환경에서 일괄보안정책 적용 인터프리터 설계 및 구현", 대전대학교 석사학위논문, 2006. 2