이기종 정보보호제품의 통합정책관리를 위한 인터프리터 설계 및 구현

홍철의°, 박진섭, 신영선, 김이곤
대전대학교
hush°@zeus.dju.ac.kr, jspark@dju.ac.kr, ysshin@zeus.dju.ac.kr, gon202@naver.com

Design and Implementation of Security Policy Interpreter for heterogeneous security products

Chul-eui Hong°, Jin-sub Park, Young-sun Shin, Yi-gon Kim
Daejeon Univ.

요 약

조직의 네트워크를 관리하기 위해 기관이나 단체에서는 다양한 보안관리 시스템을 운용하고 있다. 그러나 보안관리 시스템은 기능과 설정방법등이 서로 달라 외부의 공격에 대응하기에는 어려움이 많다. 이러한 문제점을 해결하기 위해 본 논문에서는 여러 보안관리 시스템에 정책이 일관되고, 신속하게 적용될 수 있는 인터프리터를 제안한다. 안한 시스템을 네트워크 관리에 적용할 경우 관리자가 보안관리 시스템의 특별한 설정방법을 숙지하지 않고도 정책을 신속하고 일관되게 적용할 수 있어 외부의 공격으로부터 내부 네트워크를 보다 안전하게 보호할 수 있을 것이다.

1. 서 론

세계적인 규모와 품질의 초고속 통신 인프라를 기반으로 각종 인터넷 서비스는 비약적으로 성장하고 있으며, 세계 각국의 기업들은 자사의 신기술에 대한 실험의 장으로 우리나라를 선택하고 있는 실정이다. 그러나 2003년도에 있었던 SQL 서버의 취약점을 이용한 '슬래머(Slammer)웜'의 확산은 우리나라 뿐만 아니라 전 세계 인터넷망이 영향을 받은 초유의 사태가 발생하였다. 이러한 사고를 극복하기 위해서는 보안기술과 관리체계를 통합하여 대응하여야 한다.

본 논문에서는 보안기술과 관리체계를 통합하는 한 방법으로 보안관리 시스템에 정책을 일괄적으로 적용 가능한 인터프리터를 제안하여 보안관리 시스템을 통합관리할 수 있는 방법에 대하여 제안한다. 제안한 인터프리터를 보안관리 시스템에 적용 시 외부의 공격에 대응하기 위해 각각의 설정방법을 숙지하지 않고도 신속하고, 일관된 정책을 유지하여 대응할 수 있을 것이다.

2. 기술동향

2.1 취약성의 실태

미국 카네기멜론대학의 CERT Corrdination Center의 연구보고에 의하면, 1998년 한해동안 262개만의 소프트웨어 보안 취약성이 보고되었으나 2002년 한해동안 4129개의 소프트웨어 보안 취약성이 보고되었다. 또한 과거에 비해 보안 취약점이 발표된 이후 이를 이용한 인터넷 웜이 발생하는 시간이 점점 짧아져, 보안취약점이 발견되자 마자 피해가 발생하는 "제로데이"의 실현가능성이 현실로 나타날 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

이러한 취약점을 해결하기 위해서는 본 논문에서 제안하는 능동적 네트워크 보안관리 시스템을 통해 보안정책을 수립하여 외부로부터 내부의 취약점을 보호할 수 있다.

2.3 국외 동향

OPSCE(Open Platform for Security)은 Check Point Software Technologies, Inc.가 제안하고 있는 표준으로 전사적인 보안환경을 제공하는 것을 1차적 목적으로 하고 있다. OPSEC에서는 CVP(content vectoring protocol), UFP(URL filtering protocol), SAMP (suspicious activity monitoring protocol) 등 자체 통합용 프로토콜과 LEA (log export API), ELA(export logging API), UAM (export logging API) 등의 API로 구성되어 되어 있다. Active Security는 Network Associates, Inc.가 개발한 자율적 중앙관리 보안모델로 단일 관리 시스템인 이벤트 오케스트라를 두어 사건 수집, 로그 관리, 보안 제품들에 대한 통합적 보안 정책 실행 지시 등을 중앙 집중적으로 수행한다. 이 모델은 보안관련 사건 및 문제점들을 진단하여 감시 동작을 수행하는 센서의 역할이 핵심 개념으로서, 센서는 전달된 사건을 분석, 보안정책에 따라서 대응 행동 방식을 결정한다.

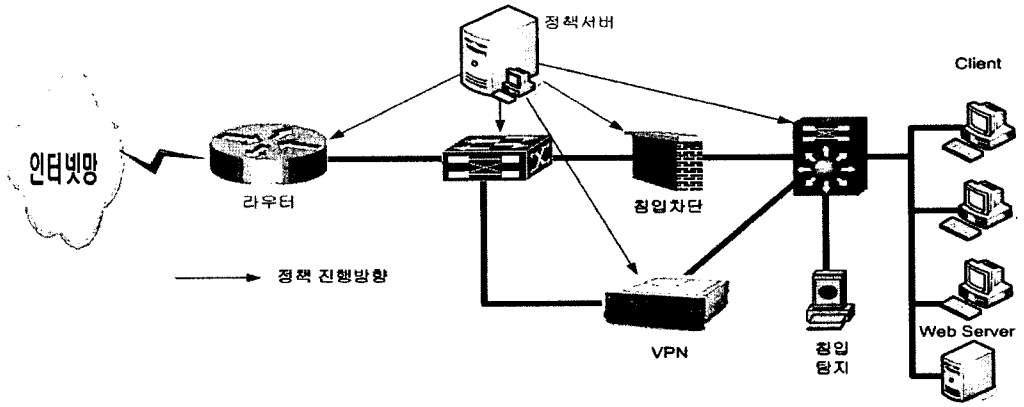

그림 1 네트워크 구성도

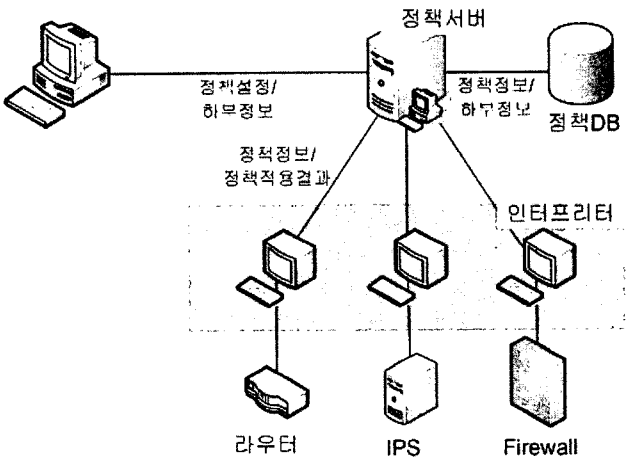

그림 2 시스템 흐름도

2.4 국내 동향

국내에서는 2003년 5월 현재 인터넷 보안기술포럼에서 EMS 표준화에 대한 작업이 이루어지고 있으나 개발업체에서는 보안제품의 통합차원에서만 이루어지고 있다.

이러한 다양한 활동에도 불구하고 이러한 조직의 대부분은 자사 위주의 개발과, 로그의 수집에 대한 통합만이 이루어지고 있다.

3. 일괄정책 적용이 가능한 통합 인터프리터

본 논문에서 제안하는 정보보호제품에 일괄정책 적용이 가능한 인터프리터는 하나의 네트워크로 구성되어 있는 대규모 네트워크 환경이나 보안관리 시스템이 원거리에 분포되어 있는 경우에 적합한 보안정책 관리기능을 제공한다. 다양한 정보보호제품으로 구성되는 네트워크는 체계적인 시스템 관리가 가능한 네트워크 환경이어야 한다.

3.1 통합 인터프리터의 구성

통합 인터프리터의 구성은 정책 관리서버, 정책 DB, 정책서버, 인터프리터, 정보보호제품으로 구성된다.

- 정책 관리서버 : 정책관리서버에서는 정책을 정해진 형식에 맞도록 정책을 설정하는 기능을 수행한다. 그리고 정책서버에 저장되어 진 하부노드에 대한 정보를 확인 할 수 있다.
- 정책DB : 정책 데이터베이스에서는 네트워크 내에 구성되어있는 정보보호제품의 종류와 각 정보보호제품에 적용할 Global 정책, 그리고 네트워크 정보를 저장한다. 이때 정책 데이터베이스에 저장되는 Global 정책은 모든 정보보호제품에 적용할 수 있는 일정한 형태로 저장된다.
- 정책서버 : 정책서버에서는 정책 관리서버에서 작성된 정책을 수신하여 이를 각각의 보안관리 시스템에 하달해 주는 서버로서, 정책 프로토콜을 통하여 하부에 있는 인터프리터에 하달하게 된다. 특히 정책서버에서는 정책관리서버로부터 신규정책이 수신되었을 경우, 이를 정책DB에 저장된 정책과 비교 검색한다. 검색시 기존정책과 충돌이 발생하면 일정한 룰에 의해 정책을 수정하여 인터프리터 및 정보보호제품에 적용하게 된다.
- 인터프리터 : 인터프리터에서는 정책서버로부터 정책 프로토콜을 이용하여 수신한 정책을 각각의 정보보호제품에 적용하는 모듈로서, 인터프리터에서는 정보보호제품의 정책을 설정하는 형식에 맞도록 정책프로토콜의 내용을 변환한다. 각각의 정보보호제품에 맞는 별도의 인터프리터를 필요로 한다.
- 정보보호제품 : 정보보호제품은 정책을 수신하여 네트워크에 적용하는 하위단계로서, 기존에 제품화되어있는 침입차단 시스템, Router, VPN 등 다양한 네트워크 정보보호제품이 이에 포함된다. 본 논문에서 제안하는 시스템은 별도의 네트워크 정보보호제품의 통합모듈을을 개발하지 않고, 기존에 사용되고 있는 정보보호제품을 활용하도록 하여 장비의 활용률을 높이도록 한다.

3.2 기능설계

가. 보안관리 시스템의 정책 자동 적용

정책 관리서버에서 생성된 정책은 정책 하달서버를 통해 각각의 보안관리 시스템에 전달이 되게 되는데, 하달된 정책은 각각의 보안관리 시스템 앞에서 정책 적용서버가 수신하여 보안관리 시스템에 입력 가능한 형태로 정책을 변환하게 된다. 이러한 기능은 관리자가 모든 보안관리 시스템의 설정방법을 숙지하지 않고도 보안관리 시스템를 제어 할 수 있으며, 또한 모든 보안관리 시스템에 대해 보안정책을 일괄적으로 적용할 수 있는 장점이 있다.

나. 보안정책의 충돌 해결

정책 관리서버에서 작성한 정책이 이미 수립된 정책과 비교하여 정책 간에 충돌이 발생하였을 경우 우선순위가 높은 정책을 적용하여 보안관리 시스템에서 적용되는 정책 간에 충돌이 발생하지 않도록 해야 한다.

3.3 인터프리터의 구현

본 논문에서 제안한 인터프리터의 설계에 의해 구현하였다.

[표 2]에서는 정책서버에서 정보보호제품에 정책을 삽입하기 위해 작성된 형식이다. 표에서 보는바와 같이 정책이 관리서버로부터 전달받으면, 이 정책을 기존의 정책과 확인한 후 데이터베이스에 저장하고, 이에 맞는 하부의 인터프리터에 전달한다. [표 3]은 정책서버로부터 정책을 수신하여, 하부에 있는 라우터에 정책을 입력하는 내용을 볼 수 있다. 여기에서 보면 상위로부터 전달받은 정책이 라우터의 정책에 맞도록 변환되어 장비에 전달되는 것을 볼 수 있다.

```
[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 CAMF data...
-----------------------------------------------
POLICY      : DenyTCP25
COMMAND     : insert
DOMAIN      : DomainServerA
DIRECTION   : incoming
ACTION      : deny
SRC ADDR    : 203.237.140.48 ~ 203.237.140.48
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( '', 'DenyTCP25',
'DomainServerA', '', '-1', '1001', '4005', '4101', '5000', '5',
'7002', '-1', '-1', '1001', '3002', '2001', '', '6000',
'203.237.140.48', '203.237.140.48', '-1', '-1', '', '', '110',
'110', '', '')
```

[표 2] 정책서버에서 생성된 정책로그

[표 4]는 동일한 정책서버로부터 정책을 수신하여 방화벽(인터프리터)에 맞는 형식으로 정책을 변환한 것을 볼 수 있다.

```
Request hdr len: 12 , camf size: 1
camf recv byte = =288
========RECV CAMF==============
        (3298|3209798304) CAMF ID:-1
        (3298|3209798304) SRC1 ADDR:203.237.140.48
        (3298|3209798304) SRC2 ADDR:203.237.140.48
        (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...
Send Command : enable
Send Command : cisco
Send Command : config terminal
Send Command : no access-list 100
Send Command : access-list 100 deny tcp 203.237.140.48
0.0.0.0 any eq 110
Send Command : access-list 100 permit ip any any
Send Command : interface serial 0
Send Command : ip access-group 100 in
```

[표 3] 라우터에 적용되는 정책(인터프리터)

```
Request hdr len: 12 , camf size: 1
camf recv byte = =288
========RECV CAMF==============
        (3298|3209798304) CAMF ID:-1
        (3298|3209798304) SRC1 ADDR:203.237.140.48
        (3298|3209798304) SRC2 ADDR:203.237.140.48
        (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 203.237.140.48 -d 0.0.0.0 -p
tcp -m tcp --dport 110 -j DROP
System : /sbin/iptables -A INPUT -s 203.237.140.48 -d
0.0.0.0 -p tcp -m tcp --dport 110 -j DROP
```

[표 4] 방화벽에 적용되는 정책(인터프리터)

4. 결론 및 향후 연구방향

본 논문에서는 정보보호제품에 정책을 일괄적용 할 수 있는 인터프리터를 제안하였다. 제안하는 시스템은 네트워크의 정보보호제품에 정책을 적용할 경우 발생할 수 있는 정책의 충돌과 신속한 대응을 할수 없다는 문제점을 해결고자 하였다.

본 시스템이 적용되면, 관리자는 정보보호제품에 대해 자세히 알지 못해도 일관된 정책을 하달하여 전체 네트워크의 보안을 향상시킬 수 있을 것이다.

향후에는 정책 관리서버에서 정책을 하달하였을 경우, 이를 정보보호제품에 적용할 수 있는 정책적용서버(인터프리터) 혹은, 모든 보안관리 시스템에 적용 할 수 있는 프로토콜의 기준이 마련되어 동일한 환경에서 다수의 정보보호제품에 정책을 하달 할 수 있는 환경이 구축되어야 할 것이다.

5. 참고문헌

[1] 김지홍, "정보보호전문가 II 네트워크 보안", 이에듀넷닷컴, 2002

[2] Ofir Arkin, "ICMP Usage in Scanning", 2000

[3] Nortel Networks, "Inverse Multiplexing for ATM Guide", 2002