제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

신뢰관리 개념의 사이버공격대응시스템 적용에 관한 연구

최명렬*, 김기한*, 이진석*
*국가보안기술연구소
e-mail: {mrchoi, ghkim1, jinslee}@etri.re.kr

A Study on Applying Trust Management Principle to Cyber Attack Response System

Myeongryeol Choi*, Gihan Kim*, Jinsuk Lee*
*National Security Research Institute

요 약

컴퓨터 시스템에 대한 해킹, 바이러스, 인터넷-웜 등을 이용한 사이버 공격의 급속한 증가는 사이버 공격 정보를 수집□ 분석하여 대응하는 사이버공격대응시스템에 대한 연구를 촉진하였다. 현재 사이버공격대응시스템의 구성 요소 중 사이버 공격 정보를 종합하여 분석하는 분석센터와 분산되어 있는 침입탐지 센서들 사이의 침입 정보교환 표준은 IETF IDMEF 로 표준화되고 있으나, 분석센터의 공격 분석 결과를 바탕으로 계속되는 공격을 차단하기 위해 침입차단시스템에 새로운 보안 정책을 교환하는 방법에는 상용 제품들이 사이의 상호 연동 인증에 사용되는 OPSEC 등이 존재하지만 아직 많은 연구가 이루어지지 않고 있다.

본 논문에서는 분석센터가 침입차단시스템에 새로운 보안 정책을 하달하고, 침입차단시스템에서 보안 정책을 집행하는 데 일관된 방법을 사용할 수 있도록 신뢰관리시스템을 사이버공격대응시스템에 적용하는 방안을 제시하고 이를 기존 방법들과 비교 분석한다.

1. 서론

현대 사회에서 인터넷이 일상 생활을 영위하기 위한 중요한 사회 기반 시설로 자리잡음에 따라 다른 사회 기반 시설과 마찬가지로 그에 대한 안전성, 가용성이 보장되지 않을 경우 사회 전체적으로 많은 불편을 끼침은 물론, 심각한 경우 국가 기능 유지에 커다란 장애를 초래하게 되었다.

과거 취미로 또는 자신의 기술을 자랑하기 위해서 행해지던 컴퓨터 시스템에 대한 공격은 최근 들어 점점 조직적, 체계적인 형태를 띄며 위험성이 날로 증가하고 있다. 특히, 인터넷-웜이나 DDoS 공격 등에 의한 피해는 짧은 시간에 전 지구적인 범위에서 영향을 주고 있을 정도로 공격 기술이 고도화되고 있다.

이러한 컴퓨터 시스템에 대한 공격에 대응하기 위한 노력의 일환으로 침입차단시스템(firewall), 침입탐지시스템(IDS) 등 공격 대응 도구들이 개발되어 사용되고 있으나 이들 단독으로는 공격 대응에 한계가 있으므로 서로 연동되어 사용되고 있다. 즉, 조직, 국가적인 차원에서 조직화, 체계화, 고도화되고 있는 사이버 공격에 대응하기 위해 네트워크에 산재해 있는 침입탐지 센서(침입차단시스템)에서 탐지된 사이버 공격 징후를 분석센터에서 종합 분석하여 상위 수준에서 공격 여부를 판단하고 이에 대응하기 위해서 침입차단시스템이나 라우터에 새로운 보안정책을 하달하는 사이버공격대응시스템에 대한 연구가 활발하게 진행되고 있다. 이때 네트워크에 산재한 침입탐지시스템, 침입차단시스템, 라우터 등이 서로 다른 종류의 시스템일 수 있으므로 이들과 분석센터 사이에 표준화된 정보 교환 방법이 필요하다.

침입탐지 센서와 분석센터 사이의 침입 정보 교환 표준으로는 IETF idwg 워킹 그룹에서 표준화하고 있는 IDMEF(Intrusion Detection Message Exchange Format)[1]가 표준으로 자리잡아가고 있으나, 분석센터와 침입차단시스템 사이의 보안 정책 교환에 대한 연구는 많이 이루어지지 않았다. 현재 사용되고 있는 방

법으로는 침입탐지시스템의 로그나 경고를 주기적으로 검사하여 침입차단시스템의 필터링 규칙을 갱신하는 방법, 상용 보안 제품들 사이에서 상호 연동을 보장하는 OPSEC 등이 있으나, 확장성과 고수준의 보안 정책을 표현, 배포, 집행하는 데는 한계가 있다. 따라서 본 논문에서는 이를 해결하기 위한 방안으로 보안 정책 표현 및 해석에 일관된 방법을 제공하는 신뢰관리 개념을 사이버공격대응시스템에 적용할 것을 제안하고 이를 기존 방법들과 비교 분석한다.

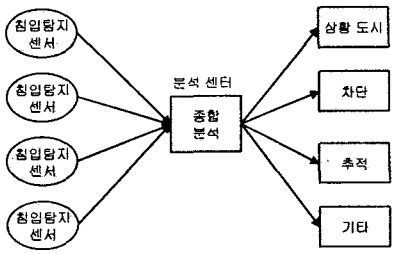
본 논문은 2 장에서 사이버공격대응시스템에 대해서 살펴보고, 3 장에서 신뢰관리시스템에 대해서 알아본다. 4 장에서 신뢰관리시스템을 사이버공격대응시스템에 적용하기 위한 방안과 기존 방법들을 비교 분석하고, 5 장에서 결론을 맺는다.

2. 사이버공격대응시스템

컴퓨터 시스템에 대한 초기 공격은 해커에 의한 원격 침투, DoS 공격, 백도어를 이용한 공격 등 단순한 형태로, 이러한 공격 들에 대한 대응책으로 침입차단시스템이 고안되어 효과적으로 이들 공격을 차단할 수 있었다. 그러나 침입차단시스템은 미리 설정된 차단 규칙에 따라 외부 네트워크와 내부 네트워크 사이의 비정상적인 트래픽을 효과적으로 차단할 수 있지만 새로운 공격 형태나 다른 호스트에서의 공격에는 대응할 수 없는 단점이 있다. 즉, 침입차단시스템의 차단 규칙은 악의적인 공격이 항상 특정 호스트 또는 호스트 그룹에서 특정 포트를 통하여 이루어진다는 단순한 가정을 하고 있다. 그러나 실재 컴퓨터 시스템에 대한 공격은 이전과는 다른 호스트를 경유하여 이루어질 수도 있고, 기존과는 다른 포트를 통하여 공격을 시도할 수 있다. 이러한 공격을 탐지하기 위해서는 특정 호스트/포트를 통한 트래픽의 존재 여부 대신에 트래픽의 내용을 바탕으로 특정 공격이 시도되고 있는지 판단하여야 한다. 이를 위하여 침입탐지시스템이 개발되었다.

침입탐지시스템의 침입탐지 결과는 공격 또는 공격으로 의심되는 행위를 하는 호스트에 대한 정보를 가지고 있으므로 이 정보는 침입차단시스템에 의해 현재 수행중인 공격 호스트로부터의 접속을 차단하는 규칙에 이용될 수 있다. 더구나 최근 들어 컴퓨터 시스템에 대한 공격 기법이 점점 고도화됨에 따라 기존 단일 시스템 또는 단일 환경에서 침입탐지 기능을 제공하던 침입탐지시스템들로는 침입 여부를 판단할 수 없는 공격 기법들이 나타나고 있다. 이에 따라 조직 또는 국가 차원에서 대규모 네트워크를 대상으로 한 공격을 탐지하기 위해서 여러 침입탐지시스템(센서)에서 제공하는 침입 탐지 정보를 종합, 분석하여 상위 수준에서 침입 여부를 판단한 후 이를 대응에 이용하는 사이버공격대응시스템 개발의 필요성이 대두되어 연구개발이 수행되고 있다. 사이버공격대응시스템의 개략적인 구조는 (그림 1)과 같다. 분석센터는 여러 침입탐지시스템들의 침입탐지 정보를 분석, 가공하여 이 정보를 바탕으로 현 침입상황 도시, 침입 호스트 또는 네트워크로부터의 연결 차단, 침입 호스트 추적 등의 처리를 수행한다. 최근 들어 다수의 침입정보를 바탕으로 상위 수준의 침입 징후를 판단하기 위한 연구가 활발히 진행 중이다.

서로 다른 종류의 침입탐지시스템과 침입차단시스템이 이러한 구조에 적용되기 위해서는 분석센터와 각종 정보를 주고 받을 수 있는 프로토콜 및 메시지 포맷이 정의되어야 한다.



(그림 1) 사이버공격대응시스템 구조

침입탐지 센서와 분석 센터 사이의 메시지 표준으로는 XML 을 탐지결과 표현 언어로 사용하는 IDMEF 가 인터넷 표준으로 추진되고 있다. IDMEF 메시지는 크게 침입탐지시스템에 의해 탐지된 침입과 그와 관련된 정보로 구성되는 경고 메시지와 침입탐지시스템 자체에 대한 정보를 주기적으로 전송하는 허트비트 (heartbeat) 메시지가 있다.

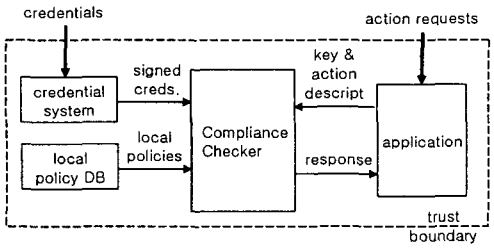
3. 신뢰관리시스템

3.1 신뢰관리, 신뢰관리시스템

일반적으로 보안 정책 집행은 보안과 관련된 행위의 수행 요청을 인증과 접근 통제의 결합으로 처리한다. 즉, 요청을 수신한 시스템은 우선 요청이 누구에 의해서 요청된 것인지 결정하기(인증) 위해 인증서(certificate)를 검사하고, 서명자가 요청된 행위를 수행하기 위해 필요한 자원에 대한 접근 권한이 있는지를 결정(접근 통제)하기 위해서 내부 DB 를 검색한다.

이에 비해 신뢰관리[2]는 보안 정책, 증명서(credential), 관계(relationship)를 표현하고, 해석하는 통일된 방법을 제공하며, 이름과 암호키를 결합시키는 인증서와 달리 증명서를 이용하여 보안과 관련된 중요한 행위에 대한 권한을 직접 위임할 수 있기 때문에 서명된 요청이 보안 정책에 부합되는지를 증명서를 이용하여 직접 결정할 수 있게 해주는 새로운 개념이다.

신뢰관리의 구조는 (그림 2)와 같다. 신뢰관리를 이용하는 응용은 요청된 보안 관련 행위를 신뢰관리가 제공하는 표현 방법을 이용하여 기술한 후 이를 요청자의 키와 함께 순응검사기(compliance checker)에 제출한다. 순응검사기는 신뢰관리가 제공하는 방법으로 표현된 지역 정책과 증명서를 바탕으로 제출된 키를 가진 사용자가 해당 행위를 수행할 수 있는 권한이 있는지 검사하여 결과를 응용에 제공한다. 응용은 이 결과를 바탕으로 요청된 행위의 인가를 결정한다.



(그림 2) 신뢰 관리 구조

신뢰관리시스템은 신뢰관리 개념을 구현한 것으로서 응용에 보안 정책과 증명서를 하기 위한 표준화된, 일반적인 메커니즘을 제공한다. 각 응용의 보안 정책은 각 응용별로 독특한 내용이지만 동일한 표기법을 이용하여 기술될 수 있으므로, 신뢰관리시스템은 보안 정책의 내용과 보안 정책 표기법, 보안 정책 검사 메커니즘을 분리하기 위해서 신뢰관리시스템을 이용하는 모든 응용들에게 표준 보안 정책 검증 메커니즘을 제공한다. 즉, 신뢰관리시스템은 응용에게는 보안 정책 집행에 필요한 보안 관련 행위의 보안 정책 순응 결과를 얻을 수 있는 표준 인터페이스를 제공하고, 사용자에게는 어떤 행위가 허용되고 어떤 행위가 불허되는지를 통제하는 데 사용되는 보안 정책과 특정 행위에 대한 권한 위임에 사용되는 증명서를 작성하는 데 사용되는 표준 언어를 제공한다. 신뢰관리시스템을 사용하게 되면 모든 응용들에게 표준화된 인터페이스가 제공되기 때문에 현재와 같이 응용 개발자가 별도의 보안 검증 메커니즘을 설계 및 구현할 필요가 없게 되고, 사용자들은 정책을 지정하는 데 유연하고 표준화된, 응용에 독립적인 언어를 이용할 수 있게 되는 장점이 있다.

3.2 KeyNote 신뢰관리시스템

대표적인 신뢰관리시스템에는 신뢰관리의 개념을 처음 소개한 PolicyMaker 와 이를 발전시킨 KeyNote[3] 등이 있다. KeyNote 는 OpenBSD 의 IPSec 구현에 사용[4]되는 등 실질적으로 사용 가능한 시스템이다. 이 시스템에서 보안 정책과 증명서를 기술하기 위해서 사용하는 KeyNote 언어[5]는 현재 RFC 2704 에 기술되어 있다.

KeyNote 는 소규모에서 대규모에 이르는 다양한 인터넷 기반의 응용에 잘 적용될 수 있도록 설계된 시스템으로, 동일한 언어를 이용하여 지역 정책과 증명서를 기술할 수 있게 해 준다. KeyNote 에서는 정책과 증명서를 통틀어 어서션(assertion)이라고 하는데, 어서션은 특정 공개 키 소유자(주체)에게 허용되는 신뢰할 수 있는 동작(행위)을 기술한다. 신뢰할 수 없는 네트워크를 통하여 전송될 수 있는 서명된 어서션은 '증명서 어서션'이라고 하는 데, 정책과 동일한 표기법을 이용하여 표현되며, 신뢰를 위임하는 주체에 의해서 서명된다. 증명서 어서션은 인증서의 역할을 할 수도 있다.

KeyNote 언어를 이용하여 권한 위임을 하기 위해서 증명서를 기술하는 예는 다음과 같다. 우선 다음과 같은 정책이 기술되어 있는 것을 가정한다.

```
Authorizer: "POLICY"
Licensees: "DSA:1f203faa2badb11ffe"
Conditions: application = "network"
            && (protocol == "tcp" || protocol == "udp")
```

이 정책은 Licensees 에 지정된 키를 가지는 주체는 Conditions 에 지정된 조건을 만족하는 어떤 행위라도 할 수 있게 허용한다. 이 정책을 바탕으로 Licensees 에 지정된 키를 가진 주체가 자신의 권한을 위임하는 경우의 예를 보면 다음과 같다.

```
Authorizer: "DSA:1f203faa2badb11ffe"
Licensees: "DSA:3a5dff3a654090abd"
Conditions: source == "192.11.255.255"
            && dest == "135.205.89.255";
Signature: "093a3134ffa3817220033110a2bc"
```

앞의 정책에서 기술된 키를 가진 주체(이 경우 Authorizer 에 키가 지정되어 있음)는 Licensees 에 지정된 키를 가진 주체에게 자신의 조건(정책에 표현되어 있는 조건)과 이 증명서에 표현된 조건을 모두 만족하는 행위를 할 수 있도록 권한을 위임하고 있다.

4. 신뢰관리 개념의 사이버공격대응시스템 적용 방안

4.1 침입탐지 로그로부터 침입차단 규칙 도출

이 방법은 단일 호스트 상에서 침입탐지 로그를 분석하여 분석된 결과로부터 해당 호스트의 침입차단시스템의 차단 규칙을 변경하는 것으로서 현재 Linux 상에서 운영되는 Perl 로 제작된 DSLI(Dynamic snort log 2 iptables)[6]와 BlockIt[7]이라는 도구가 공개되어 있다. 이들은 모두 공개 침입탐지 도구인 snort 의 로그 파일 또는 경고의 내용을 주기적으로 읽어 침입을 시도하는 호스트로 분석된 새로운 호스트가 로그 파일에 나타나면 해당 호스트를 차단하는 규칙을 Linux 커널의 침입차단기능인 iptables 의 룰셋(ruleset)에 등록하는 방법을 사용한다.

이 방법은 기능이 상대적으로 단순하기 때문에 구현과 사용이 쉬운 장점이 있지만, 침입차단 규칙을 별도의 프로그램이 직접 변경하기 때문에 단일 호스트 상에서 운영되어야 하며, 특정 도구에만 적용 가능한 단점이 있다.

4.2 OPSEC

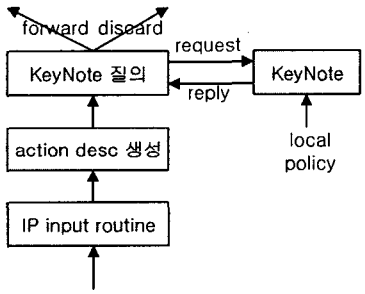
OPSEC(Open Platform for Security)[8]은 체크포인트사가 제정한 표준으로 침입탐지시스템, 침입차단시스템, VPN, 방화벽 제품 등 정보보호 관련 제품들 사이의 상호운용성을 보장하는 여러 가지 프로토콜 및 API 의 집합이다. 정보보호 제품 개발 업체는 자사 제품을 체크포인트 사에 의뢰하여 표준을 만족하는지 인증을 받는다. 인증을 받은 제품들 사이에는 상호운용이 가능하다. 이중에서 침입탐지시스템과 침입차단시스템 사이의 연동 표준은 SAM(Suspicious Activity Monitoring)으로 이 표준에 따라 개발된 침입탐지시스

템은 체크포인트사의 VPN-1/FireWall-1 제품과 연동되어 특정 네트워크나 호스트로부터 침입으로 의심되는 행위가 탐지되면 이 표준을 이용하여 해당 연결 차단과 지정된 시간 동안 해당 네트워크나 호스트로부터의 연결 시도를 차단하도록 침입차단시스템에 차단 규칙을 지정할 수 있다.

이 방법은 상용 표준으로 규격이 공개되지 않아 공개 침입차단시스템에 적용이 불가능한 단점이 있다.

4.3 신뢰관리 개념 적용

사이버공격대응시스템의 분석센터와 침입차단시스템 사이의 보안 정책 교환에 신뢰관리 개념을 적용하기 위해서는 이들 사이에 안전하게 보안 정책을 전달할 수 있는 통신 방법이 제공되어야 한다. 보통 IPSec 등 안전한 통신 채널을 이용하여 전달하지만, 서명된 증명서는 FTP 등 안전하지 않은 경로를 이용할 수도 있다. 신뢰관리는 보안 정책 표현방법과 검증 메커니즘을 제공하므로 신뢰관리를 이용하는 침입차단시스템은 신뢰관리시스템을 이용하도록 침입차단 처리과정이 변경되어야 한다. KeyNote 신뢰관리시스템을 이용하는 침입차단시스템의 침입차단 처리 과정을 (그림 3)에 나타냈다.



(그림 3) 신뢰관리시스템을 이용한 침입차단 구조

침입차단시스템은 네트워크 인터페이스로부터 수신된 IP 패킷의 주소 및 포트 정보로부터 패킷이 수행하려고 하는 동작에 대한 action description 을 생성하여 신뢰관리시스템에 보안 정책 검증을 요청하면 신뢰관리시스템은 분석센터에서 수신된 지역 정책과 action description 을 바탕으로 정책 검증 결과값을 돌려주고, 침입차단시스템은 이 결과값을 조사하여 적절한 처리를 한다.

분석센터에서 침입차단시스템으로 하달하는 차단 규칙에 해당하는 보안 정책을 KeyNote 언어로 기술한 예는 다음과 같다.

```
Authorizer: "POLICY"
Conditions: app_domain == "firewall"
            && remode_addr == "198.001.004.001"
            && local_port == "80" -> "discard";
```

이 예에서는 198.1.4.1 호스트에서 임의의 80 포트로 접속을 요청하는 패킷에 대해서 폐기할 것을 지정하고 있다.

신뢰관리시스템을 사이버공격대응시스템에 적용하기 위해서는 기존 침입차단시스템의 침입차단 처리루틴을 변경해야 하는 단점이 있지만, 신뢰관리 언어는 프로그래밍 언어처럼 확장성이 있기 때문에 임의의 보안 정책을 표현할 수 있고, 신뢰관리 언어와 정책 검증 메커니즘이 표준화되어 있기 때문에 보안 관련 응용들이 동일한 보안 정책 표기법과 검증 메커니즘을 이용할 수 있어 동일한 방법을 안전한 통신 연결 협상[4], 침입차단시스템, 인증시스템, 웹서버 등 다양한 응용에 이용할 수 있는 장점이 있다.

신뢰관리 개념의 사이버공격대응시스템 적용과 관련된 주된 장점은 사이버공격대응시스템이 조직, 국가 차원의 공격 및 공격시도를 탐지하기 위해서 다단계로 구축될 경우 최상위 수준에서 결정되는 보안 정책을 적용하기가 쉽다는 점이다. 최상위 수준의 보안 정책은 고수준의 언어로 기술되는데 다른 방법들에서는 이를 침입차단시스템에 그대로 적용하기 어렵지만 신뢰관리의 경우 STRONGMAN[9] 프로젝트에서 연구되고 있는 것처럼 상위수준의 표현을 KeyNote 언어 등을 중간언어로 번역하는 기법을 이용하면 그대로 적용 가능하게 된다.

5. 결론

이상으로 사이버공격대응시스템에서 공격 분석 결과에 따라 새롭게 결정된 보안 정책을 침입차단시스템에 하달하여 집행하기 위한 새로운 방법으로 신뢰관리 개념을 이용하는 방안을 제시하고 이를 기존 방법들과 비교 분석하였다. 보안 정책 표현, 배포, 집행에 신뢰관리시스템을 이용하게 되면 동일 보안 정책 표기법과 보안 집행 메커니즘을 보안 관련 응용에 사용할 수 있으므로 확장성이 뛰어난 장점이 있다. 향후 고수준으로 기술된 보안 정책을 신뢰관리시스템 언어로 번역하는 기술 등에 대한 연구가 진척이 있을 경우 조직, 국가적 차원의 보안 관리에 손쉽게 적용할 수 있을 것으로 판단된다.

참고문헌

[1] IDMEF, http://www.ieft.org/internet-draft/draft-ietf-idwg-idmef-xml-07.txt
[2] M. Blaze, etc., The Role of Trust Management in Distributed Systems Security, Lecture Notes in Computer Science (Vol. 1603 - Secure Internet Programming), pp. 185-210, Springer-Verlag Inc., 1999.
[3] The KeyNote Trust-Management System, http://www.cis.upenn.edu/~keynote/
[4] M. Blaze, etc., Trust Management for IPSec, The Internet Society Symposium on Network and Distributed Systems Security (SNDSS) 2001, 2001.2.
[5] M. Blaze, etc., The KeyNote Trust Management System Version 2, RFC 2704, 1999. 9.
[6] Dynamic snort log 2 iptables , http://www.ncwald.de/dsli
[7] BlockIt , http://blockit.teknofx.com
[8] http://www.opsec.com
[9] STRONGMAN, http://www.cis.upenn.edu/~strongman