통합보안관리시스템을 위한 보안정책 일반화에 관한 연구

최 현 희† · 정 태 명††

요 약

이기종 보안 제품들을 통합관리하기 위한 통합보안관리시스템은 보안관리를 위한 불필요한 보안정책의 중복을 피하고 보안 제품들을 효율적으로 상호운용하기 위해 제안된 보안관리 구조이다. 본 논문에서는 보안 제품들에 대한 다양한 보안정책 관리 구조들을 통합된 형태로 보안적으로 무결한 보안정책을 설정할 수 있는 보안정책 일반화 관리 구조를 제안한다. 보안정책 일반화의 목적은 네트워크 상에서 존재하는 모든 보안 시스템들에 대한 보안관리의 효율성, 편의성 보장과 보안성 향상에 있으며, 이질적인 보안 정책제어 구조를 수용할 수 있도록 하는 것이다. 보안정책 일반화 과정은 관리자의 보안목표와 보안요구사항 설정, 각 보안제품과 보안 에이전트들에 의해 수집된 정보들에 대한 분석을 통하여 보안상태를 확인하며, 위험요소에 대한 보안정책 적용 방법들을 보안목표와 보안요구사항, 보안정책목록 정보를 기준으로 적절성을 판별하는 일련의 과정으로 정의할 수 있다. 보안정책 설정과정의 일반화는 이기종 보안정책에 대한 통합관리가 가능하게 하며, 보안 정책간의 충돌 및 중복 설정과 같은 일관성 문제를 해결함으로써 보안정책의 무결성을 보장하고, 네트워크 상에서 존재하는 보안제품의 제어에 편의성을 제공한다.

A Study on Generalization of Security Policies for Enterprise Security Management System

Hyun H. Choi† · Tai M. Chung††

ABSTRACT

Enterprise security management system proposed to properly manage heterogeneous security products is the security management infrastructure designed to avoid needless duplications of management tasks and inter-operate those security products effectively. In this paper, we propose the model of generalized security policies. It is designed to help security management build invulnerable security policies that can unify various existing management infrastructures of security policies. Its goal is not only to improve security strength and increase the management efficiency and convenience but also to make it possible to include different security management infrastructures while building security policies. In the generalization process of security policies, we first diagnose the security status of monitored networks by analyzing security goals, requirements, and security-related information that security agents collect. Next, we decide the security mechanisms and objects for security policies, and then evaluate the properness of them on the basis of security goals, requirements and a policy list. With the generalization process, it is possible to integrate heterogeneous security policies and guarantee the integrity of them by avoiding conflicts or duplications among security policies. And further, it provides convenience to manage many security products existing in large networks.

키워드 : 보안정책(security policy), 정책관리(policy management), 통합보안관리(enterprise security management)

1. 서 론

대규모 네트워크 상에서 다수의 보안시스템이 설치되어있을 경우, 네트워크 전반에 걸쳐 보안상황을 파악하고 많은 수의 다양한 보안 정책들 간의 무결성을 보장하는 것은 상당히 어려운 작업이다[1, 2, 12]. 각 보안시스템마다 별도의 관리자를 배치한 경우에도 각 관리자 간의 원활한 정책 의견교환과 의사소통이 필요하나 이러한 과정을 거쳐 정책이 적용되기까지는 불필요한 시간과 노력이 필요할 뿐만 아니라, 잘못된 의사소통이나 관리자의 실수로 인해 네트워크 보안정책에 치명적인 결함을 가질 수도 있다.

최근 들어, 네트워크의 보안성 향상을 위하여 이미 실용화되어 실제 적용되고있는 침입탐지 및 침입차단 시스템, 가상사설망 등과 같은 보안 제품군들은 기술적으로 성장단계에 있으며, 이와 더불어 이러한 보안 제품군들을 관리하기 위한 보안관리구조 역시 빠르게 발전하고 있다.

그러나, 이러한 보안관리 구조들은 다양한 보안 제품군들이 갖고 있는 기능적 공통점을 일반화하여 보안정책에 반영

† 준 회 원 : 성균관대학교 대학원 전기전자 및 컴퓨터공학과
†† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2002년 3월 27일, 심사완료 : 2002년 8월 21일

하기 보다는 단순히 UI(User Interface)의 통합만을 제공하여 관리 작업을 한 곳에 집중시켜 오히려 관리자의 부담을 가중시키고 있다. 그리고, 보안 제품군들이 갖고 있는 특정 파라미터를 통한 보안정책 설정이나, 통합관리를 위한 보안 제품간의 연동성에 보다 중점을 둠으로써 보안관리를 보다 복잡하게 만드는 경향이 있다. 이와 같은 보안관리구조가 보다 광범위한 네트워크에 적용될 경우, 보안관리의 복잡도를 증가시킴으로써 관리의 어려움은 더욱 심각해 질 것이다.

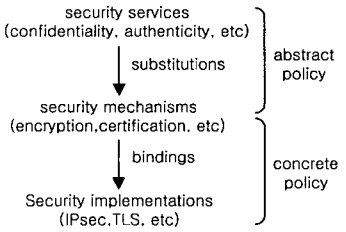
보안정책의 일반화는 앞서 제시된 문제점들을 해결하기위한 것으로써, 대규모 네트워크상에서의 통합보안관리 수행을 위해 반드시 요구되는 부분이다. 보안정책의 일반화 과정을 통해 통합 보안관리 구조는 다양한 보안 제품들 사이에 존재하는 기능적 공통점을 보안정책에 반영함으로써, 보안정책의 복잡도를 제거할 수 있다. 또한, 각각의 보안 제품들을 운용하기 위하여 큰 문제로 제기됐던 보안 정책들 간의 충돌 및 중복 설정을 배제할 수 있기 때문에 통합보안정책의 크기를 간소할 수 있다는 장점을 갖는다. 뿐만 아니라, 각 보안 제품들 또는 관리 에이전트들에 의해 수집된 정보를 유기적으로 공유할 수 있기 때문에 각 보안 제품들 또는 관리 에이전트들에 의하여 수집된 보안 관련 정보들은 통합 분석과정을 거쳐 일반화된 보안정책에 반영되고, 설정된 보안 정책들은 각 보안 제품들에 재반영 됨으로써, 보안 제품간의 연동성을 크게 향상시킬 수 있다.

본 논문에서는 대규모 네트워크상에 분산 설치되어 있는 다수의 보안 제품들을 통합관리하기 위하여 현재 연구하고 있는 보안정책 일반화 과정에 대하여 소개한다. 본 논문의 구성은 2장을 통하여 통합 보안관리 구조에 관한 연구 동향에 대해서 기술하며, 3장에서는 보안정책 일반화 과정에 대하여 기술한다. 마지막으로 4장에서는 본 연구를 통하여 추출된 결론과 향후 연구 방향에 대해서 언급하고자 한다.

2. 연구 동향

현재 네트워크 보안관리구조는 침입탐지시스템, 침입차단시스템, 가상사설망 등과 같은 공격의 근원지를 찾아내고 차단하는 기능을 가진 하부조직에 속하는 보안 시스템들을 중앙 집중적으로 통합 관리하는 방향으로 지속적인 연구가 진행되고 있다[3-5, 12].

최근 연구활동으로는 통합 보안정책의 동적관리를 위한 MSME(Multidimensional Security Policy Management for Dynamic Coalitions)가 있다. MSME 시스템은 SAL(Security Abstraction Layer)에 기반하고 있으며, MSME SAL은 ISO 보안구조(ISO 7498-2)의 일부분과 ISO 7498-2에서 정의되지 않은 서비스와 메커니즘을 추가적으로 포함하고 있다. 추가적으로 포함된 것으로는 coalition members와 steganography mechanism 사이의 통신서비스를 들 수 있다. SAL에서 정책관리자들은 특정한 보안을 독립적으로 이행함으로써, 상위레벨 보안서비스에 관하여 판단과 계획을 세울 수 있다.



(그림 1) Abstraction Levels

(그림 1)은 MSME에 대한 추상적인 개념을 도시한 것이다. MSME 시스템은 어떠한 보안 메커니즘으로 보안 서비스를 제공할 것인지를 결정하고, 결정된 보안 메커니즘의 구현 기술을 결정하여 동적으로 연결 구성함으로써 보안정책을 동적으로 구성 관리할 수 있다. 예를 들어, (그림 1)에서 MSME 시스템이 특정 네트워크에 기밀성 서비스를 제공하기위해 암호화 메커니즘을 사용할 것을 결정하였다면, IPsec의 DES 또는 Triple-DES 암호화 알고리즘, TLS의 Triple-DES 또는 RSA 등과 같은 구현 기술을 통하여 기밀성 서비스를 제공할 수 있다. 그러나, MSME에서 제안된 이론이 실용화 되기 위해서는 보안 서비스를 제공하기 위해 설정된 보안 정책들이 보안 메커니즘을 정확히 받아들이는지에 대한 모니터링 기능과 정책 적용의 자동화 기능이 필요하다[5].

현재 활용되어지고 있는 대표적인 통합 보안관리 구조로는 SVN(secure virtual network)이 있다. SVN은 Checkpoint사의 Firewall-1/VPN-1 제품을 중심으로 사용자 인증 시스템, 정책관리 시스템이 통합된 enterprise network 보안 환경으로서, SVN을 구성하는 각각의 보안 제품들을 통해 IP기반의 enterprise network의 모든 시스템을 보호할 수 있다. SVN은 OPSEC(Open Platform Security)을 통하여 SVN 환경내의 보안 제품들간의 상호 동작성과 통합을 지원 받으며, OPSEC은 SVN을 더욱 안전한 환경이 되도록 지원한다.

OPSEC은 각 보안 시스템들간의 개입 없이 자동적인 보안관리를 목적으로 하며, 전체적으로는 각 보안시스템의 독립적인 고유 기능을 수행하면서 상호협력 한다는 면에서 분산보안시스템의 성격을 갖고 있다. 그러나 OPSEC의 경우 통합보안기능을 적용하기 위해 도입 가능한 보안제품군이 Checkpoint사 제품과 Checkpoint사가 제시한 표준을 통해 구현된 제품들로 한정된다는 단점을 갖고 있다[6-8].

또 다른 통합 보안관리 구조로는 Network Associates사의 Active security시스템이 있다. Active security시스템의 구조를 살펴보면, 개념적으로 보안과 관련되는 이벤트를 탐지하는 시스템인 센서(sensor), 보안사건에 대응을 하는 시스템

인 행위자(actor), 그리고 이들의 행위를 중재하고 조율하는 중개인(arbiter)으로 구성되어 있다. OPSEC과 달리 중개인이라는 존재를 두어 정책과 각 보안 관련 사건의 수집 및 사건들에 대한 행위를 중앙에서 제어하는 기능을 갖는 중앙 집중적 보안시스템으로 정의된다. 그러나 현재 이를 지원하는 제품군은 다양하지 않으며, Network Associates사의 보안 제품들간에서만 상호연동을 지원하는 단점을 갖고 있다[9, 10].

본 논문에서 제안하는 통합보안관리 시스템을 위한 보안정책 일반화는 이기종 보안 제품들에 대한 통합관리에서 자사 보안제품 또는 주도적인 단체나 회사가 제시한 표준을 통해 구현된 제품들간에서만 상호연동을 지원하던 한계성을 극복할 수 있다. 또한, 보안관리상의 불필요한 정책 중복 설정을 피할 수 있으며, 다양한 보안 제품들을 효율적으로 상호운용할 수 있는 기능을 포함하는 관리구조로 정의할 수 있다.

3. 보안정책 일반화

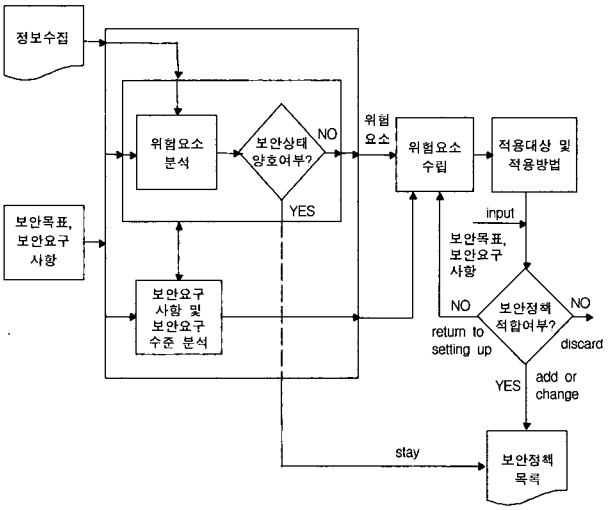
보안정책 일반화는 통합보안관리의 기반으로서, 모든 보안 시스템들에 대한 보안관리의 효율성, 편의성 및 보안성 향상을 목적으로 하며, 보안 시스템들 간의 상호연동이 가능하도록 보안정책을 구성할 수 있다.

보안정책의 일반화란 각 보안 제품들 마다 독립적으로 보유하고 있는 특정 파라미터를 통하여 보안정책을 설정하는 것이 아니라, 보안 제품들의 기능적 공통점을 일반화하여 보안정책에 반영하고, 보호대상 네트워크로부터 수집된 보안 관련 정보에 대한 분석 결과를 일반화된 보안정책의 설정과정에 반영함으로써 보안 제품들 간의 연동성과 보안정책관리의 효율성을 향상시킬 수 있는 보안정책관리 모델이다. 그리고, 보안정책 일반화 과정을 통하여 보안정책의 중복 및 충돌현상을 미연에 방지할 수 있기 때문에 보안정책의 무결성을 향상시킬 수 있다.

3.1 보안정책 일반화 과정

보안정책 일반화 과정은 우선 네트워크 상에서 발생할 수 있는 정보들을 수집하는 작업으로부터 시작된다. 수집된 정보들과 초기 설정된 보안목표, 보안요구사항을 바탕으로 위험요소를 분석하고, 분석된 결과를 통하여 보안상태를 파악하게 된다. 한편, 수집된 보안 관련 정보들은 보안목표, 보안요구사항과 함께 보안요구사항 및 보안요구수준 분석과정에 이용되며, 분석 결과는 보안정책 수립을 위한 정보로 제공된다. 분석과정을 통해 추출된 결과를 토대로 일반화된 보안정책을 수립하고, 정책 적용을 위한 적용대상 및 적용방법을 결정한 후, 보안정책 방안들의 무결성 보장을 위해 보안정책 적합여부 판별과정을 통하여 수립된 보안정책의 적합성을 판단한다. 설정된 보안정책이 적합할 경우 보안정책목록에 보안정책이 추가 또는 변경되며, 적합하지 않을 경우 수집된 정보들을 바탕으로 보안정책 재설정 혹은 폐기된다.

(그림 2)는 위에서 설명한 보안정책 일반화 설정과정을 도시한 것이다. (그림 2)에서 나타난 바와 같이, 보안정책 일반화 과정은 특정 보안시스템을 위한 정책구조에 국한되지 않을 뿐만 아니라, 이러한 일반화 구조는 통합 보안관리 구조에 유연성을 향상시킨다.



(그림 2) 보안정책 일반화 과정

3.1.1 정보수집 단계

네트워크 상에서 발생하는 정보들은 각 보안 제품들 또는 관리 에이전트들에 의해 수집되며, 수집된 정보들은 특정 보안시스템을 위한 분석에 국한되지 않고 통합 분석된다.

침입탐지 및 침입차단시스템, 가상사설망, 취약성진단시스템 등의 보안 제품들은 네트워크나 시스템의 사용 형태를 실시간 감시 또는 보호함으로써 보안 관련 정보를 수집한다. 보안 제품들로부터 허가되지 않은 사용자로부터의 접속, 정보의 조작, 오용, 남용 등에 대하여 수집된 정보들은 각 보안 시스템들에 의해 보고된 보안위반 사건들간의 관련성을 파악하고, 보안 시스템들의 운용을 위하여 요구되는 보안 정책들 간의 일관성 유지를 위해 통합 분석된다.

3.1.2 보안목표 및 보안요구사항 설정 단계

관리자에 의해 초기에 설정된 보안목표와 보안요구사항은 위험요소 분석과 보안요구사항 및 보안요구수준 분석과정에 적용된다. 또한 이는 다양한 위협에 노출되어 있는 보안적용대상에 대한 보안정책 설정의 적합여부를 판별하는 기준이 된다.

초기 보안목표와 보안요구사항은 보안대상 네트워크상에 존재하는 보호대상 객체들에 대한 관리자의 보안요구수준을 고려하여 작성되며, 보안성 이외에도 보안제품 운영과 관련된 관리기능, 상호연동기능 등과 같은 다양한 요소들을 고려하여 보안정책에 반영될 수 있도록 작성되어야 한다.

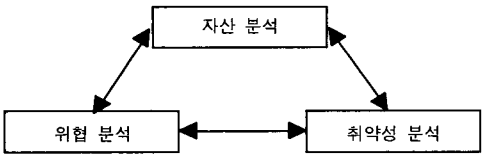
3.1.3 위험요소 분석 단계

보안대상에 포함되는 사용자들의 자산에 대한 평가를 기준으로 무엇으로부터 보호할 것인지 결정한다. 모든 보안대상의 위험요소 분석을 위한 고려사항으로는 자산의 인지도, 자산의 유용성, 자산의 가용성, 사건발생 잠재성, 접근가능성, 법 집행 효율성, 억제력 등이 있다.

〈표 1〉 보안대상의 위험요소 분석을 위한 고려사항

고 려 사 항	설 명
자산의 인지도	자산의 존재가 외부에 알려져 있는 정도
자산의 유용성	자산의 금전적 가치 및 손실 시 피해정도
자산의 가용성	자산의 희소성 및 다른 곳에서의 사용가능정도
사건발생 잠재성	위협이 발생할 가능성 및 확률
접근가능성	보안시스템의 체계에 따른 접근 용이도
법 집행 효율성	준법정신 및 법 집행기관의 효율성
억제력	위협 목적 달성 후 도피의 난이도

자산에 대한 위험요소로는 사고/재난, 도난/침입, 방화/화재, 자연재해, 정보침해, 독극물/가스, 폭력, 테러 등이 있다. 네트워크 상에서 발생될 수 있는 위협요소로는 데이터 또는 파일의 삭제, 복사, 수정, 운영체계 취약점, 서비스 거부, 응용 프로토콜 취약점, 바이러스, 도청, 데이터 위변조, 프로토콜 취약점, 트래픽 폭주 등이 있다.



(그림 3) 위험요소 분석

위험요소 분석은 자산 분석, 위협 분석, 취약성 분석의 상호관계를 바탕으로 위험요소를 추출하는 것이다. 자산 분석이란 네트워크 상에 발생되는 모든 자산을 파악하고, 각 자산의 가치 및 중요도를 산출하는 과정이다. 위협 분석이란 자산에 피해를 가할 수 있는 잠재적인 요소인 위협을 파악하고 발생 가능성 등을 분석하는 과정이다. 취약성 분석은 자산 분석을 통하여 도출된 자산의 속성과 중요도를 바탕으로 자산이 근본적으로 가지고 있는 약점인 취약성을 발굴하고 취약성이 전체적인 위험에 미칠 수 있는 영향을 분석하는 과정이다.

다음 식을 통하여 위험요소를 산출한다.

$$RV(Risk\ Value) = AV(Asset\ Value) \times REL(Risk\ Exposure\ Level) \times TC(Threat\ Cycle)$$

AV와 TC는 자산 분석과 위협 분석으로부터 산출하여 적용된다. RV는 TC의 영향으로 변동폭이 크므로, TC의 산출 시 최근 1년 이내를 기준으로 한다. REL은 아래 두 가지 경우에 따라서 다르게 산출된다.

모든 위협들로부터 자산에 대한 위험가치 산출시 :

$$REL = \sum severity\ levels\ of\ threats\ on\ a\ object \quad (1)$$

각 위협들 마다 자산에 미치는 위험가치 산출시 :

$$REL = severity\ levels\ of\ threat \quad (2)$$

식 (1)과 식 (2)로부터 자산의 취약성 정도와 각각의 자산에 위협을 가하는 위험요소들을 산출할 수 있다.

3.1.4 보안요구사항 및 보안요구수준 분석 단계

보안관리의 분류는 크게 물리적, 관리적, 기술적 측면으로 분류되며, 보안요구사항 및 보안요구수준을 분석하는 기준 중 하나이다. 보안관리에 대한 분류는 <표 2>와 같다.

〈표 2〉 보안관리 분류

보안관리의 분류	보안관리 종류
물리적 보안관리	물리적 보안과 환경 보안 인사 보안 비즈니스의 연속성 관리
관리적 보안관리	통신과 작동 관리 부합성
기술적 보안관리	액세스 관리, 인증 무결성, 암호화 시스템 개발과 유지보수

보안요구사항 및 보안요구수준 분석 단계에서는 정보자산에 대한 적절한 분석을 하기 위하여, 보호의 필요성, 우선순위 그리고 보안 정도 등에 따른 분류를 통하여 분석을 한다. 일반적으로 자산가치를 산정하는 방법에는 크게 정량적 방법과 정성적 방법 두 가지가 있다. 정량적 방법은 정보자산에 대해 위협발생확률과 잠재적 손실크기를 곱해서 이를 화폐가치로 환산하여 위험의 정도를 측정하여 정보자산을 평가하는 방법이다. 정성적 방법은 정보자산에 대해 위협발생으로 인한 손실크기를 화폐가치가 아닌 기술변수로 나타내는 손실측정 방법이다. 자산들중 정보자산의 경우 속성상 화폐단위로 환산 하기가 매우 어려우므로, 본 논문에서는 정성적 방법을 가지고 자산을 평가 하도록 한다. 자산을 정성적인 방법으로 <표 3>과 같이 보안요구(보호의 필요성, 우선순위, 보안정도 등) 수준을 크게 5등급으로 나누어 분류한다.

〈표 3〉 보안요구수준 분류

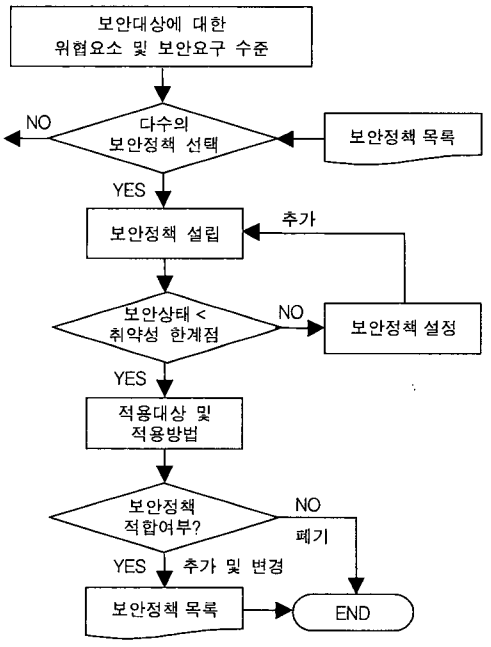
등 급	설 명
Very High(Scale : 5)	가장 높은 경우
High(Scale : 4)	비교적 높은 경우
Medium(Scale : 3)	보통인 경우
Low(Scale : 2)	그다지 낮지 않은 경우
Very Low(Scale : 1)	가장 낮은 경우

분석된 보안요구사항 및 보안요구수준에 대한 보안정보에 따라 보안정책 방식이 차별화 된다.

3.1.5 보안대상 및 보안정책 적용방식 추출 단계

보안목표와 위험요소, 보안요구사항 및 보안요구수준 분석 과정의 결과를 통하여 보안정책 적용대상과 보안정책 적용방법을 추출한다. 여기서 보안정책은 하나의 보안사건에 대해 여러 개의 보안정책 적용 방식들이 추출될 수 있다.

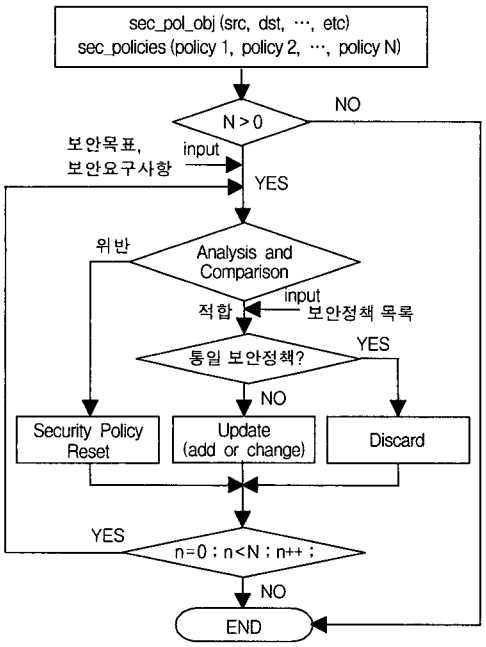
통합보안관리시스템 혹은 관리자는 보안대상에 대한 위협요소 및 보안요구수준 정보를 기반으로 보안정책목록에 저장되어있는 보안 정책들 중 다수의 보안정책을 선택하게 된다. 선택된 보안 정책들은 설립시 보안상태 여부를 판별 받게 된다. 보안상태가 강화된 경우 선택된 보안정책은 적합성 여부 판별과정을 거치게 된다. 반면, 보안상태가 취약한 경우 관리자에 의해 보안정책이 추가되어지며, 보안상태 판별과정으로 되돌아가게 된다. 추가된 보안정책 설정으로 보안상태가 강화된 경우 통합보안관리시스템 및 관리자에 의해 설정된 보안 정책들은 보안정책 적합여부 판별과정을 통하여 적합할 경우 추가 혹은 변경처리 되어지며, 부적합 할 경우 폐기처리 된다. (그림 4)는 보안대상 및 보안정책 적용방식 추출과정을 나타낸 것이다.



(그림 4) 보안대상 및 보안정책 적용방식 추출과정

3.1.6 보안정책 적합성 판별 단계

제시된 보안 정책들은 각 보안정책마다 보안정책 적합성 여부를 평가 받는다. (그림 5)는 설정된 보안정책의 적합여부를 판별하는 과정이다. 먼저, 첫 번째 보안정책을 관리자가 초기에 설정한 보안목표와 보안요구사항에 대한 적합여부를 판별하고, 적합할 경우에는 보안정책목록과의 비교를 통하여 동일 보안정책 여부를 판별한다. 동일 보안정책일 경우, 제시된 보안정책은 폐기 처리된다. 동일 보안정책이 아닐 경우, 보안정책은 보안정책목록에 추가 또는 변경된 보안정책을 적용시킨다. 관리자가 설정한 보안목표와 보안요구사항에 위반될 경우에는 보안정책 설정과정으로 되돌아간다. 이후 차기 보안정책들은 동일한 판별과정을 통하여 적합성 여부를 판정 받는다.



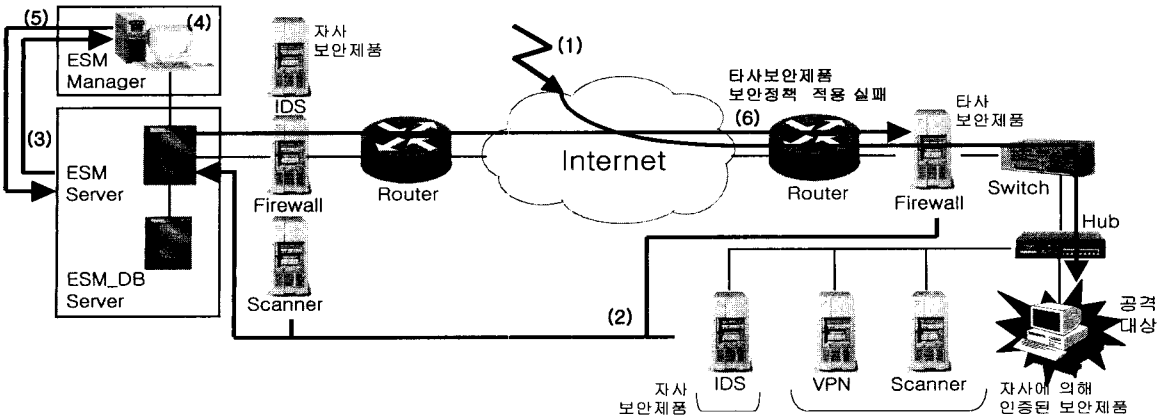
sec_pol_obj : 보안정책 대상 정보들
sec_policies : 보안정책 적용 방법들
N : 입력된 보안정책 적용 방법의 총 개수

(그림 5) 보안정책 적합여부 판별과정

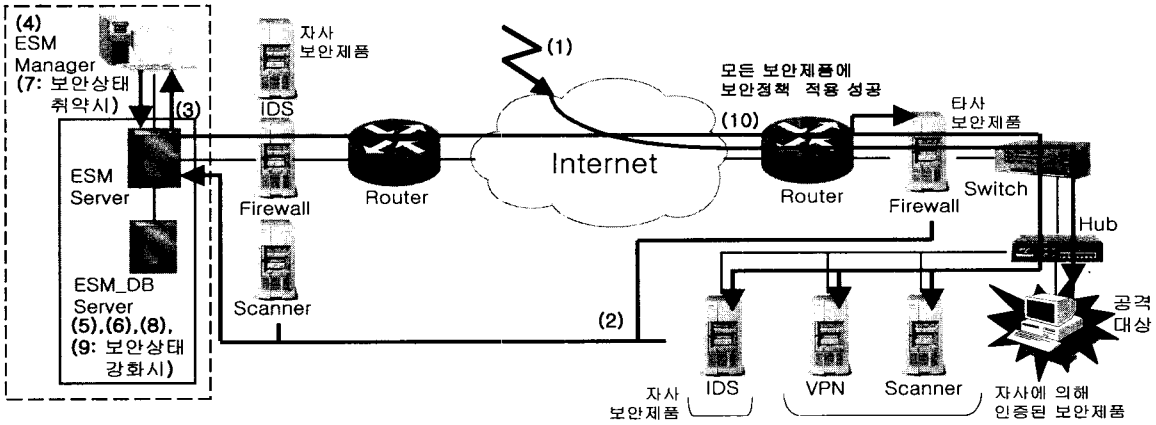
예를 들어, 동일 보안대상 적용에 대한 중복 설정여부의 판단을 위하여 적용 대상간의 포함관계를 고려할 수 있다. 하나의 네트워크 세그먼트 내에 존재하는 호스트들은 해당 네트워크에 포함되며, 현재 해당 네트워크에 대한 보안정책이 적용되고있다면, 네트워크에 포함되는 호스트에 대하여 적용하고자 하는 보안정책이 네트워크 보안정책에 위배되는 경우 부적합한 것으로 판정된다.

3.2 적용 예제 및 비교 분석

본 논문에서 제시한 통합보안관리시스템에서의 일반화된 보안정책 관리구조에서의 보안정책 설정과정과 현존의 보안정책 관리구조에서의 보안정책 설정과정을 간단한 적용 예를 통하여 비교 분석해 보고자 한다. (그림 6)은 네트워크 상에서의 일반적인 통합보안관리에서의 보안정책 설정과정을 도시한 것이며, (그림 7)은 본 논문에서 제시된 통합보안관리에서의 일반화된 보안정책 설정과정을 도시한 것이다.



(그림 6) 일반적인 보안정책 설정과정



(그림 7) 일반화된 보안정책 설정과정

일반적인 통합보안관리에서의 보안정책 설정과정

1) 공격자가 한 호스트에 보안위협을 내포하고 있는 서비스 제공.
2) 통합보안관리시스템을 통해 각 보안 제품군들 혹은 관리 에이전트들에 의해 수집된 보안 관련 정보들이 통합관리 됨.
3) 통합보안관리시스템으로부터 관리자 웹 인터페이스에 보안정보 제공.
4) 관리자는 인터페이스를 통해 제공되어지는 정보(로그, 모니터링 정보 등)와 자동대응(E-mail, 알람 등) 등을 바탕으로 위험 분석.
5) 위험 분석 결과 위험발생시 관리자로부터 특정 파라미터를 사용한 보안정책 설정.
6) 관리자에 의해 설정된 보안정책을 받은 통합보안관리시스템에서 정책 적합여부 과정을 통하여 적합 시 보안정책 적용 및 변경, 부적합 시 보안정책 폐기.

단, 보안정책은 한번에 하나의 보안정책만 설정할 수 있으며, 그리고 자사제품 혹은 자사가 제시한 표준을 통해 구현된 제품만 보안정책 적용이 가능하다. 이러한 가장 큰 이유 중 하나는 보안제품에 대한 특정 파라미터 값을 사용해 보안정책을 설정하기 때문이다.

본 논문에서 제시된 통합보안관리에서의 일반화된 보안정책 설정과정

1) 공격자가 한 호스트에 보안위협을 내포하고 있는 서비스 제공.
2) 통합보안관리시스템을 통해 각 보안 제품군들 혹은 관리 에이전트들에 의해 수집된 보안 관련 정보들이 통합관리 됨.
3) 통합보안관리시스템으로부터 관리자 웹 인터페이스에 보안정보 제공.
4) 통합보안관리시스템에서 수집된 보안정보와 관리자에 의해 설정된 보안목표 및 요구사항을 바탕으로 위험 분석 혹은 관리자가 인터페이스를 통해 제공되어지는 정보(로그, 모니터링 정보 등)와 자동대응(E-mail, 알람 등) 등을 바탕으로 위험 분석.
5) 위험발생시 통합보안관리시스템으로부터 다수개의 보

안정책 설정.

6) 보안정책 설정시 취약성 분석.
7) 분석 결과 보안위험 한계점을 초과할 경우 관리자를 통한 새로운 보안정책 추가, 한계점에 미달할 경우 보안정책 수렴.
8) 보안정책 추가시 재평가.
9) 분석 결과 보안위험 한계점을 넘을시 6과 7의 과정 반복설정, 한계점에 미치지 않을 경우 보안정책 적합 판별 확인.
10) 보안정책이 적합할 경우 보안정책 추가 혹은 변경, 부적합 할 경우 보안정책 폐기.

그러나 위험발생시 반드시 통합보안관리시스템으로부터 보안정책 설정 후 보안상태 판별과정에서 나온 결과 취약성 문제가 발생하였을 경우에만 관리자가 보안정책을 설정하는 것은 아니다. 관리자는 통합보안관리시스템으로부터 웹 인터페이스상으로 제공된 보안정보를 바탕으로 위험 분석 결과를 가지고 언제든지 보안정책을 설정할 수 있다. 관리자는 보안제품 종류에 따른 특정 파라미터를 기반으로 보안정책을 설정하거나 또는 보안요구사항 및 보안목표 등의 보안관련 정보 추가 설정을 하게 된다. 추가 설정된 정보를 바탕으로 통합보안관리시스템에서는 보안정책을 설정한다. 그리고 관리자가 보호대상에 대한 보안서비스를 통합보안관리시스템에 요청하였을 경우 통합보안관리시스템에서는 요청된 보안서비스를 실행시킬 수 있는 다수개의 보안 제품들을 선별하여 보안정책을 설정한다.

3.3 일반화된 보안정책의 구조적 특징

본 논문에서 제안하는 보안정책 일반화 과정은 다음과 같은 구조적 특성을 갖는다.

- 다양한 보안 제품군들이 갖고 있는 기능적 공통점을 일반화하여 보안정책에 반영한다.
- 일반화된 보안정책을 통해 보안 제품들 유기적인 상호연동이 가능하다.
- 보안정책 간의 충돌 및 불필요한 중복 설정을 피할 수 있다.

우선, 보안정책의 일반화는 다양한 보안 제품군들이 갖고 있는 기능적 속성과 동작의 공통점을 묶어 일반화하여 보안정책에 반영해 준다는 장점을 갖는다. 보안정책 일반화는 보안제품군들이 좀 더 효율적으로 상호운용을 할 수 있도록 해주는 방법으로써, 보안 제품간의 상호운용을 통하여 자동대응 기능을 지원하며, 보안정책 설정에서의 일관성과 편의성을 향상시킨다.

둘째로, 보안정책의 일반화 과정은 각 보안 제품 혹은 에이전트들로부터 수집된 보안 관련 정보의 통합 분석과정을 통하여 수립되기 때문에 다수의 보안 제품들이 타 보안 제품에 의하여 수집된 보안 정보를 공유할 수 있다. 이는 일반화 과정을 통하여 수립된 보안정책을 통하여 각 보안 제품들에 반영되기 때문에 결과적으로 보안 제품들간의 상호 연동성을 향상시킬 수 있다.

마지막으로, 각 보안 제품들이 서로 다른 관리구조를 사용함으로써 발생되는 보안 정책간의 충돌 및 불필요한 중복설정을 피할 수 있다는 장점을 가진다. 보안정책 설정에 대한 적합여부 판별을 거쳐 최종적으로 보안정책이 적용됨으로써 중복정책 설정을 막을 수 있으며, 보안정책 설정에 대한 초기 보안목표와 보안정책을 비교함으로써 좀 더 적합한 보안정책을 적용할 수 있다.

4. 결론 및 향후 계획

본 논문에서는 이기종 보안 제품들을 통합관리하기 위한 보안정책 일반화 관리구조를 제안하였다. 제안된 보안정책 일반화 관리구조는 지금까지 보안 제품들 간의 상호 연동성에 중점을 둠으로써 보안정책 관리구조의 복잡도를 증가시키고 있는 통합보안관리시스템과는 차별성을 갖는다. 기존의 통합보안관리시스템은 보안 제품군들이 갖고 있는 특정 파라미터를 통한 보안정책을 설정함으로써 다양한 보안 제품간의 연동성 문제를 야기시켰으나, 일반화된 보안 정책관리 구조는 다양한 보안 제품군들이 갖고 있는 기능적 공통점을 일반화하여 보안정책에 반영함으로써 보안 제품간의 연동성 및 관리의 효율성을 향상시킨다. 또한, 보안정책 일반화 관리구조는 새로 설정된 보안 정책들에 대한 보안정책 설정 적합여부를 보안목표, 보안요구사항 및 보안정책목록을 기준으로 한 판별 과정을 통하여 동일 정책 존재 유무, 상반 또는 위반되는 정책 유무 등을 판별하게 된다. 판별 과정에서 보안 정책간의 충돌 및 중복설정에 따른 문제점을 해결함으로써 보안정책의 무결성이 보장된다.

본 연구를 통하여 제시된 보안정책 일반화 관리구조는 보안 제품군들 또는 관리 에이전트들로부터 수집된 보안 관련 정보들에 대한 통합 분석과정을 거쳐 생성된 보안정책을 반영하고, 설정된 통합보안정책을 통하여 다수의 이기종 보안제품을 효율적으로 관리하기 위한 목적으로 연구되었으며, 대규모 네트워크 상에서 다수의 보안시스템을 관리하는 보안정책 구현에 적합하다고 사료된다. 관리자에 의해 설정된 보안목표와 보안요구사항들은 광범위한 정보를 내포하고 있으므로 예외적인 발생 상황이 나타날 수 있는 만큼 보안정책 적용방식에 대한 구체적인 연구가 필요하다.

참 고 문 헌

[1] J. Zao, L. Sanchez, et el, "Domain based Internet security policy management," DARPA Information Survivability

Conference and Exposition, 2000, DISCEX '00, Proceedings, Vol.1, pp.41-53, Jan., 1999.
[2] L. Lewis, "Implementing policy in enterprise networks," IEEE Communications Magazine, Vol.34, Iss.1, pp.50-55, Jan., 1996.
[3] D. Schnackengerg, H. Holliday, et el, "Cooperative Intrusion Traceback and Response Architecture (CITRA)," DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01, Proceedings, Vol.1, pp.56-68, Jan., 2001.
[4] R. Barruffi, M. Milano, et el, "Planning for security management," IEEE Intelligent Systems [see also IEEE Expert], Vol.16, Iss.1, pp.74-80, Feb., 2001.
[5] G. Patz, M. Condell, et el, "Multidimensional security policy management for dynamic coalitions," DARPA Information Survivability Conference & Exposition II, 2001, DISCEX '01. Proceedings, Vol.2, pp.41-54, Feb., 2001.
[6] Check Point Software Technology, Inc., Open Platform for Security (OPSEC) Technical Note, 2000.
[7] Check Point Software Technology, Inc., Check Point VPN-1/Firewall-1 OPSEC API Specification, Version 4.1, Nov., 1999.
[8] Check Point Software Technology, Inc., Secure Virtual Network Architecture, A Customer-focused White Paper, Nov., 2000.
[9] Network Associates, Inc., Automating Security management white Reducing Total Cost of Ownership, 1999.
[10] Network Associates, Inc., Active Security Getting Started Guide Version 5.0, 1999.
[11] Communications Security Establishment(CSE), Threat and Risk Assessment Working Guide, ITSG-04, Canada, Oct. 1999.
[12] D. S. Kim, T. M. Chung, "Implementation of Integrated Firewall Management System by Central Policy Management," KNOM 2000, pp.169-176, May, 2000.

최 현 희

e-mail : hhchoi@rtlab.skku.ac.kr
2001년 세명대학교 전자공학과 졸업(학사)
현재 성균관대학교 대학원 전기전자 및 컴퓨터공학과 석사과정 재학
관심분야 : 네트워크 보안, 보안 관리

정 태 명

e-mail : tmchung@ece.skku.ac.kr
1984년 일리노이주립대학교 전자계산학과 졸업(학사)
1987년 일리노이주립대학교 대학원 컴퓨터공학과(공학석사)
1995년 Purdue대학교 대학원 컴퓨터공학과(공학박사)
1995~1999년 성균관대학교 전기전자 및 컴퓨터공학부 조교수
2000~현재 성균관대학교 정보통신공학부 부교수
관심분야 : 망관리, 네트워크 보안, 통합보안 관리, 액티브 네크워크