PRISM : 보안 레이블을 이용한 위험예방 통합보안관리 모델

김 동 수† · 김 태 경† · 정 태 명††

요 약

다양한 조직들이 그들의 전산환경을 효과적으로 보호하기 위해 보안시스템을 설치하고 이들 보안 시스템들을 통합보안기술을 이용하여 관리를 하고 있는 추세이다. 그러나, 현재의 통합보안관리 모델은 수동적이며 사후 대응 방식이다. 공격성공 가능성을 낮추고 보안관리 비용과 자원의 절감을 위해서는 위험예방 차원의 보안관리가 필요하다. 본 논문에서는 정보 자산의 중요도와 자산이 위치한 호스트/네트워크의 보안성을 평가하여 사전에 자산에 대한 보호대책을 세우는 사전 준비 방식의 통합보안관리 모델인 PRISM을 제안한다. PRISM은 자산이 처리되는 호스트나 네트워크의 보안 수준을 평가한 결과에 따라서 각 보안 시스템들의 정책을 적절히 조정하고 각 자산들에게 요구되는 수준의 안전성을 확보하기 위한 보안관리 모델이다. 사전 예방 방식의 보안 관리를 실현하기 위한 PRISM은 현재와 같이 복잡한 네트워크 보안에 대한 효과적인 방법을 제시할 것이다.

PRISM : A Preventive and Risk-reducing Integrated Security Management Model using Security Label

Dong-Soo Kim† · Tae-kyung Kim† · Tai-myoung Chung††

ABSTRACT

Many organizations operate security systems and manage them using the integrated security management (ISM) technology to secure their network environment effectively. But current ISM is passive and behaves post-event manner. To reduce cost and resource for managing security and to remove possibility of succeeding in attacks by intruder, the preventive security management technology is required. In this paper, we propose PRISM model that performs preventative security management with evaluating the security level of host or network and the sensitivity level of information asset. PRISM compares the security level with the sensitivity level to decide appropriate security measures for protecting that asset from potential risks before security incidents occur. The PRISM can give concrete and effective security management in managing the current complex networks

키워드 : 보안관리(Security Management), 보안 레이블(Security Label), ESM, 통합보안관리, 전사적 보안관리

1. 서 론

현대는 소위 정보화 사회이다. 사회의 거의 모든 활동이 이들 정보를 기반으로 이루어 지고 있으며 정보들은 '지식'으로 발전되고 더욱 큰 가치를 생산해 낸다. 이들 정보의 처리와 전달은 현재 컴퓨터와 데이터 통신기술에 전적으로 의존하고 있다.

인터넷의 출현 이후 현재까지 컴퓨팅 기술과 데이터 통신기술은 눈부시게 발전하고 있다. 이러한 기술의 발전에 힘입어 컴퓨터와 데이터 통신은 대학이나 연구소 뿐만 아니라 비즈니스 영역 그리고 각 가정까지 그 보급이 점점 더 확산되고 있다. 컴퓨터와 데이터 통신은 개인과 조직들에게 편의를 제공하는 기술의 차원을 넘어 사회를 지지하는 하나의 기반으로 자리잡고 있다. 정보화 사회는 바로 이 컴퓨터와 데이터 통신의 기반 위에 존재하고 있는 것이다.

인터넷의 확산은 시공을 초월한 데이터 통신이 가능하게 하지만, 공공의 네트워크인 성격으로 다양한 악영향을 초래하기도 한다. 인터넷을 통해 형성된 사이버 공간은 익명성을 전제로 하는 사이버 범죄들이 산재하여 있는 공간이다[1]. 인터넷을 통해 전달되는 정보들은 유출과 도용의 위험에 노출되어 있으며 공격자들은 인터넷을 통해 조직의 네트워크에 접근하거나 서비스를 무단으로 이용하거나 정보의 변조, 파괴, 도용을 할 수 있다. 결국 이러한 위험을 방지하고자 다양한 보안 기술에 대한 연구가 진행되어 왔으며 침입차단시스템, 침입탐지시스템, 취약점 분석 시스템, VPN, 암호화 기술 등이 개발되어 활용되어 왔다[2-5].

정보 보안의 궁극적인 목표는 서비스나 정보의 가용성과

† 준 회 원 : 성균관대학교 대학원 정보통신공학부
†† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2003년 7월 22일, 심사완료 : 2003년 9월 16일

무결성, 은닉성 보장이다[6]. 이들 서비스와 정보 그리고 이들이 존재하는 기반 구조들을 이루는 요소-컴퓨터, 네트워크 장비-들을 조직의 자산으로 정의할 수 있으며, 이들 조직 자산의 보호가 잘 이루어 질 때 안전한 네트워크 환경을 조성할 수 있다. 보안 시스템들은 본질적으로 이들 자산을 보호하기 위한 기술이 구체화된 것이다[7].

정보보안을 위한 보안 시스템 들의 종류가 다양해 지고, 네트워크의 규모에 따라 다수의 보안 시스템들을 운영하여야 하는 상황에서 이들에 대한 관리가 또 다른 문제점으로 부각되었다. 일반적으로 보안 시스템들의 관리는 전문적인 지식을 필요로 하며, 이들의 관리를 위해서는 많은 시간과 자원을 요구한다. 따라서, 이들 다양한 보안제품의 관리와 공격에 대한 자율적인 대응이 가능하도록 하는 통합보안관리기술이 각광을 받고 있다[8-11]. 그러나, 지금까지의 통합보안 관리 기술은 사후대응 방식을 갖고 있으며, 전산 환경의 보호에만 치중하였다.

본 논문에서는 이러한 현실을 감안하여 보안 사건 발생 이전에 보다 능동적으로 자산을 보호하기 위한 통합보안관리 구조를 설명한다.

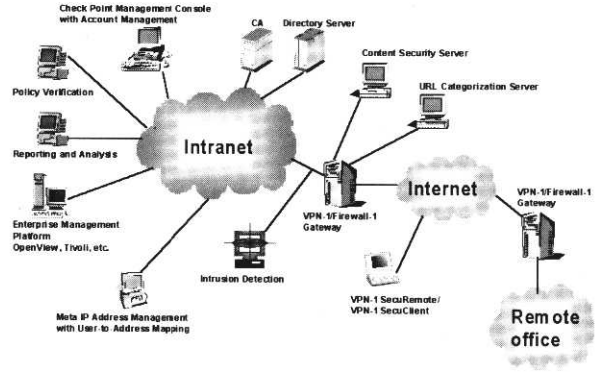
본 논문의 구성은 3장에서 PRISM의 개략적인 구조를 설명하고 4장에서 PRISM의 관리 객체들과 객체들의 관계를 설명한다. 5장에서는 PRISM의 보안관리 유형과 보안 레이블을, 6장에서는 위험예방 보안관리의 동작 절차와 평가를 기술한다. 마지막으로, 7장에서는 결론 및 향후 과제를 제시한다.

2. 통합보안관리 기술 동향

기존 통합보안 관리의 예로, 보안 산업계에서 대표적인 Checkpoin사의 SVN/OPSEC이 있으며, 이는 보안 시스템 간의 상호 협력성에 초점을 맞추고 있다[8, 9]. 한편, 보안 연구영역에서는 미국의 DARPA에서 IDIP(Intrusion Detection Isolation Protocol) 프로젝트를 시작하여 현재 보안 정책과 대응 및 공격 추적 구조를 추가한 CITRA(Cooperative Intrusion Traceback and Response Architecture)가 대표적인 통합보안관리 모델이다[10, 11]. 다음은 이들 두 통합보안 관리 모델을 설명한다.

2.1 SVN/OPSEC

SVN은 Check Point사의 방화벽-1/VPN-1 제품을 중심으로 사용자 인증 시스템, 정책 관리 시스템이 통합된 전사적 네트워크 보안 환경으로서, SVN을 구성하는 각각의 보안 제품들을 통해 IP 기반의 전사적 네트워크의 모든 시스템을 보호하기 위한 구조이다. (그림 1)은 SVN의 개략적인 구조를 나타내고 있다. SVN 환경은 게이트웨이를 보호하고, 응용프로그램 서버 수준에서 single sign-on을 지원하며, 사용자 위치에 상관없이 개별적인 접근 제어를 수행할 수 있도록 한다.



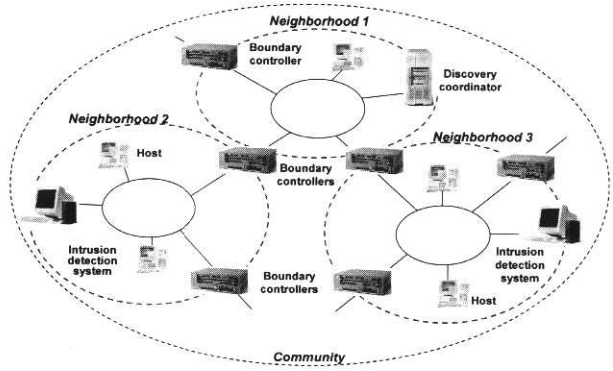
(그림 1) SVN의 개략적인 구조

OPSEC은 이러한 SVN 환경 내의 보안 제품들 간의 상호 동작성과 통합을 지원하여 SVN 환경을 구체적으로 실현하기 위한 프로토콜과 API 집합이다. 또한, OPSEC SDK를 이용하여 구현된 응용 프로그램들은 OPSEC을 통한 통신을 보호하기 위해 SSL을 이용할 수 있다.

SVN Phase II는 보안 시스템들과 eBusiness 응용 프로그램들 간에 강력한 통합기능을 제공하기 위한 보안 구조이다. 특히, B2B eBusiness 기반구조에 대한 보안을 제공하기 위하여 설계된 보안 구조라 할 수 있다.

SVN Phase II의 핵심은 Check Point사의 VPN-1 제품에 추가된 모듈인 UserAuthority API이다. UserAuthority API를 통해서 네트워크의 각 응용 프로그램들은 사용자 인증 정보를 공유할 수 있다. 사용자는 각 응용 프로그램에 대해 따로 인증 절차를 거치지 않고 응용프로그램간의 투명한 인증 절차를 거쳐 서비스를 이용할 수 있는 편리함을 제공받는다.

2.2 CITRA



(그림 2) CITRA의 구조

CITRA는 공격을 추적하여 실제 근원지를 식별하여 근원지 가까운 곳에서 공격을 차단하기 위해 네트워크 기반의

침입탐지시스템, 침입차단시스템, 라우터들을 통합하는 구조이다. CITRA에서 각 구성 요소들은 IDIP(intruder detection and isolation protocol)라는 프로토콜을 통해 상호 협력한다. IDIP는 침입의 추적 및 고립에 대한 협력작업이 가능하도록 하는 응용 계층의 프로토콜로서 침입탐지시스템, 침입차단시스템, 호스트, 보안관리 관련 요소 시스템들의 협력 하에 탐지된 침입을 추적하고 고립시키는데 필요한 정보들을 공유할 수 있도록 하는데 그 목적이 있다.

CITRA는 또한 관리자의 공격 분석 및 대응 작업을 자동으로 처리하기 위해 개발되었다. CITRA 구조와 소프트웨어 라이브러리는 공격의 분석과 대응 프로세스를 자동화하는 통합 기반구조를 구성한다. CITRA는 독립적으로 개발된 컴포넌트들을 저비용으로 통합하고 이러한 컴포넌트들의 행동을 유연하게 접목시킬 수 있도록 설계되어 있다.

CITRA는 다음과 같은 두 가지 수준의 집합으로 구성되어 있으며, (그림 2)는 이들의 구성을 나타내고 있다.

- **CITRA 커뮤니티(community)** : 하나의 탐지 조정자(discovery coordinator)라 불리는 관리 컴포넌트의 관리 도메인을 지칭한다. 다시 말해, 하나의 CITRA 커뮤니티에는 하나의 탐지 조정자가 운영된다.
- **CITRA 이웃(neighborhood)** : CITRA 커뮤니티는 상호 연결된 CITRA 이웃의 집합으로 구성된다. CITRA 이웃은 CITRA를 지원하는 서로 인접한 장치들의 집합이다. CITRA 이웃은 CITRA 구조를 구성하는 가장 기초적인 단위이다.

CITRA는 이와 같은 커뮤니티와 이웃 구조를 통해 공격의 역추적을 수행하며, IDIP를 사용하여 침입과 관련된 정보를 수집하고 공격을 역추적하며, 자동적으로 공격에 대한 대응을 수행한다.

3. 위험예방 방식의 통합보안관리 모델

통합보안관리의 1차적인 목적은 네트워크 상의 보안 시스템들을 관리 감독하는 것이며, 보안 정책을 효과적으로 분배하는 것이다[12, 13]. 각 보안 시스템들을 유기적으로 통합하여 자율적인 대응과 보안 관리동작이 이루어지도록 하는 것은 2차적인 목적이라 할 수 있다.

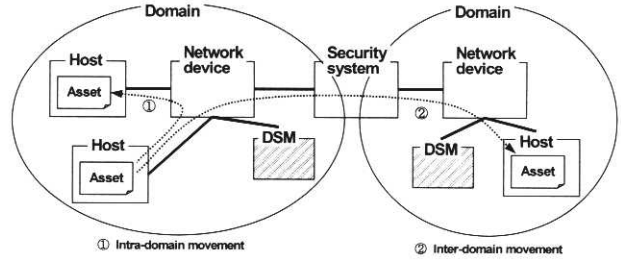
PRISM 모델은 다수 보안 시스템들에 대한 통합관리와 보안사건에 대한 자율적 대응이라는 기존 통합보안관리의 목적을 충족함과 동시에, 보안사건 발생 이전에 정보자산의 중요도에 따른 위험예방 차원의 보안관리를 가능하게 하는 것이 그 목적이다. 이는 위험분석 기술과 보안관리 기술의 접목을 통해 이루어질 수 있다.

위험분석 기술 영역에서 다양한 위험분석 기술, 방법론 및 도구들이 연구되었으나 현실적으로는 위험분석의 결과가 거의 인력에 의해 적용되고 있으며 위험분석에 따른 보안관리를 지원하는 기술과 도구는 아직까지 개발된 바가 없다.

위험분석 기술은 조직 네트워크의 취약성을 발견하고 자산에 대한 잠재적인 위협 요소들을 제거하거나 위험에 대한 적절한 대책을 수립할 수 있도록 하여 조직 네트워크 보안을 효과적으로 강화하는 데 필수적인 기술 중의 하나이다. 따라서, 위험분석 기술과 보안관리 기술의 접목을 통해 보안사건 이전에 적절한 보안조치가 취해질 수 있도록 하는 방식의 통합보안관리가 필요하다.

기존의 통합보안관리는 공격을 감지하고 관리 대상 네트워크 상의 보안 시스템들의 정책을 조정하는 수동적 대응 방식이다. 그러나, 앞으로의 통합 보안은 취약성을 사전에 파악하고 중요 자산에 대한 보호를 공격 이전에 강화하여 보안 사고를 미리 예방하는 능동적인 방식으로 바뀌어야 한다. 또한, 자산에 대한 중요도를 선별하여 보안 대응 조치 및 예방 활동을 하는 것은 관리 비용과 기타 보안 관리 활동에 필요한 자원의 낭비를 줄여 효율성을 도모할 수 있다. 따라서, PRISM 모델에서는 기존의 통합보안관리 기술을 포함하면서 중요 정보자산의 이동을 추적하고 정보자산이 처리되는 네트워크 및 호스트의 보안 수준을 평가하여 평가결과에 따라 보안 대응책을 강화함으로써 위험예방 차원의 보안 관리를 실현하는 능동적인 통합보안 관리를 제안한다.

PRISM은 보호하고자 하는 조직의 네트워크를 특징이나 용도와 함께 물리적인 경계를 고려하여 구분하고 각각의 도메인과 도메인에 속한 호스트들에 대한 보안 수준 등급을 부여한다. 그리고, 보호 대상 자산에 중요도를 부여하여 이들 정보의 비교를 통해 보안대책 적용을 판단하고 보안 시스템 정책의 재설정을 통해 보안 사건 이전에 예방 차원의 통합 보안관리를 실현한다.



(그림 3) PRISM 모델과 자산 이동 유형

(그림 3)은 PRISM 모델과 자산 이동의 두 가지 유형을 나타낸다. PRISM의 구성을 간략히 소개하면, 조직의 네트워크는 도메인으로 구분되고 도메인 내에는 도메인 보안관리자(domain security manager, DSM)가 존재하여 자신이 속한 도메인의 보안관리를 담당한다. 도메인 내의 다른 구성요소로 네트워크 노드가 있으며, PRISM 모델에서 노

드는 호스트, 네트워크 장치, 보안 시스템을 포괄하여 지칭하는 개념이다.

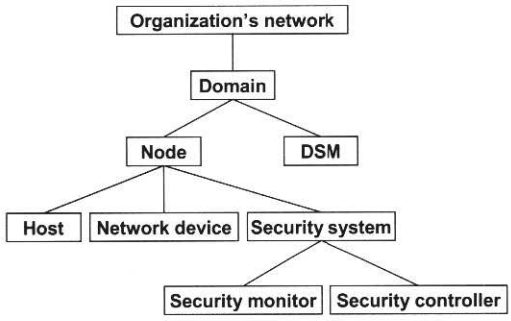
PRISM 모델에서는 관리 대상 네트워크 내에서의 자산 이동을 크게 두 가지 형태로 분류한다. 각 구성 요소들 간의 자산 이동은 크게 한 도메인 내 노드간의 이동(intra-domain movement)과 서로 다른 도메인에 속한 노드들간의 이동(inter-domain movement)으로 구분한다.

도메인 내 노드간의 자산 이동의 경우 해당 도메인의 DSM이 이의 추적과 이동에 따른 위험예방 보안 관리를 전적으로 담당하며, 도메인간 자산 이동의 경우 자산이 이동해 간 도메인의 DSM 뿐만 아니라 원래 자산이 위치해 있던 도메인의 DSM도 자산 상태 변화의 처리에 대한 보안관리를 수행한다.

4. PRISM 모델의 관리객체

본 장에서는 PRISM 모델을 구성하는 요소들인 관리 객체들과 이들의 계층 관계에 대해서 설명한다.

자산 객체는 PRISM의 구성 요소들간을 이동하며 PRISM 보안관리 모델을 통해 보호하려는 대상 객체이므로 PRISM 네트워크를 구성하는 관리 객체와는 다르게 취급된다. PRISM 모델의 관리 객체들은 계층적으로 구성된다. (그림 4)는 PRISM 구성 요소들의 계층 관계를 나타낸 것이다.



(그림 4) PRISM 모델 관리객체의 계층구조

4.1 자 산

〈표 1〉 자산의 분류

구 분	설 명	예
정보 자산 Information asset	조직 네트워크나 컴퓨팅 장치를 통해 다루어지는 가치를 갖는 전자적인 정보	인사 목록 파일 사업계획 파일
서비스 자산 Service asset	사용자에게 정보의 처리, 접근, 저장을 제공하는 기능 단위	웹 서비스 전자우편 서비스
시스템 자산 System asset	네트워크를 구성하고 서비스를 제공하기 위해 사용되는 물리적 장치	웹 서버 파일 서버

PRISM 모델에서 조직의 자산은 <표 1>과 같이 정보 자산, 시스템 자산, 서비스 자산으로 크게 세 가지 유형으로 분류된다. 이들 중 시스템 자산과 서비스 자산은 이동이 거의 없는 고정 자산으로 간주하며 정보 자산은 지속적인 복제와 이동이 이루어지는 유동 자산으로 간주한다. 한편, 정보 자산은 고정 자산들 사이에 내재될 수 있다.

PRISM 모델에서는 정보 자산의 중요도 평가 및 이들에 대한 예방 차원의 보호를 최선의 목적으로 한다. 따라서, 현 시점에서 PRISM 모델의 관리 대상 자산은 동적으로 이동과 생성, 삭제가 빈번한 정보 자산으로 제한한다.

4.2 노 드

노드는 네트워크를 구성하는 단위 요소들이며, 네트워크에 연결되어 있고, 정보자산 즉 데이터를 처리할 수 있는 능력을 가진 시스템들이다. 노드는 각기 고유의 기능을 수행하는 단위이다. 노드는 호스트, 네트워크 장치, 보안 시스템의 세 가지로 구분된다.

- **호스트** : 호스트는 조직의 네트워크에 연결되어 있으며 정보 자산을 다루거나 서비스를 제공할 수 있는 컴퓨팅 장치를 의미한다. 이의 예로는 서버, PC, 워크스테이션 등이 있다.
- **네트워크 장치** : 네트워크 장치는 네트워크 상에서 다른 컴퓨팅 장치들 간의 통신이 가능하게 해 주는 기능을 갖는 요소이다. 이의 예로는 라우터, 스위치 등이 있다.
- **보안 시스템** : 보안 시스템은 보안 기능을 수행하는 요소이다. 보안 시스템은 그 기능에 따라 크게 보안 감시자(security monitor), 보안 제어자 (security controller)의 두 가지 유형으로 분류할 수 있다. 보안 감시 시스템은 보안 사건을 탐지하거나 발견해 내기 위한 보안 시스템으로써 IDS, 취약점 분석도구를 예로 들 수 있다. 보안 제어 시스템은 보안 정책에 따라 접근제어나 암호화와 같은 제어기능을 수행하는 보안 시스템이다. 방화벽, VPN을 예로 들 수 있다. 근래 보안 시스템 구현 기술이 발전함에 따라 보안 사건을 탐지하고 능동적으로 대처하는 보안 시스템들(예 : IPS, Computer virus vaccine 등)이 출현하여 유형별 구분이 모호하므로 보안 감시기능과 보안 제어기능을 동시에 갖춘 보안 시스템의 경우 보안 감시자로 분류한다. 이에 대한 요약이 <표 2>에 나타나 있다.

〈표 2〉 보안 시스템의 분류와 예

구 분	설 명	예
보안 감시자 Security monitor	보안 사건을 탐지하고 보고하는 기능을 수행하는 보안 시스템	침입탐지시스템 취약성점검시스템
보안 제어자 Security controller	무결성, 비밀성, 가용성의 보장을 위해 특정 보안 기능을 수행하는 보안 시스템	방화벽 가상사설망시스템 호스트 접근제어시스템

4.3 도메인

PRISM 모델에서 보안 관리 대상이 되는 조직의 네트워크 영역은 물리적 경계와 네트워크의 특성, 용도에 따라 구분하여 각각의 구분된 네트워크를 도메인으로 정의한다. PRISM 모델에서 보안 수준 평가는 기본적으로 자산을 직접적으로 다루는 각 호스트들과 네트워크 수준의 보안 관리를 위해서 도메인에 대해서도 보안 수준의 평가가 이루어진다. 이는 보안 수준이 다른 도메인 사이에 자산 이동이 발생할 경우에 네트워크 수준의 보안 정책을 재 수립하기 위함이다.

도메인은 기본적으로 도메인의 보안 관리를 담당하는 도메인 관리자와 두 가지 보안 시스템을 가지고 있어야 한다. 도메인 관리자는 도메인 내에서의 자율적인 보안관리를 수행하기 위해 도메인 내의 보안 사건을 탐지하고 보안정책을 적용하는 시스템이다.

도메인은 크게 신뢰되는(조직의 제어 하에 있는) 도메인과 비신뢰적인(조직의 제어를 받지 않는) 도메인으로 분류할 수 있다. 신뢰되는 도메인은 반드시 인접할 필요는 없으며 지역적으로 원거리에 위치하고 비신뢰적인 도메인을 경유하여 도달될 수도 있다.

이러한 경우의 예로는 조직의 보안관리 권한 하에 있으나 지역적으로 떨어져 공중망을 이용하여 연결된 조직의 네트워크를 예로 들 수 있다.

비신뢰적인 도메인에서 유입되는 자산은 경계 대상이며 검사가 필요하다. 비신뢰적인 도메인에서 유입되는 자산은 그 자체에 악성 코드를 포함하고 있을 수 있으며, 그 내용을 신뢰할 수 없고, 조직 네트워크 보안에 치명적인 피해를 줄 가능성이 존재한다. 또한, 조직 자산이 비신뢰적인 도메인으로 유출되는 경우를 철저하게 감시하여야 하며, 비신뢰적인 도메인을 경유하여 자산이 이동되는 경우에는 이동 경로에 대한 보안 대책이 이루어져야 한다. 즉, 자산 이동의 최종 목적지가 타 신뢰되는 도메인이라 할 지라도 비신뢰적인 도메인을 경유하여 이동되므로 비신뢰적인 도메인에서의 보안 위협에 대한 대책을 수립하여야 한다. 이를 위한 보안 대책의 대표적인 예로는 데이터 암호화, SSL, VPN, PGP 등이 있다.

4.4 도메인 보안 관리자

도메인 보안 관리자(DSM)는 한 도메인의 통합보안관리를 수행하는 필수 구성 요소이다. 보안 감시 시스템은 보안사건의 발생을 도메인 관리자에게 통지하고, 도메인 관리자는 사건의 유형과 보안 정책에 따라 보안 제어 시스템을 위한 정책을 생성하고 적용한다. 즉, 도메인 관리자와 두 가지 유형의 보안 시스템을 통해 도메인 내부에서의 자율적인 사후대응 방식의 통합보안관리가 이루어진다.

5. PRISM의 보안관리와 보안 레이블

본 장에서는 PRISM 모델에서 수행되는 보안 관리 유형을 분류하고 이들 각 유형에 대한 세부 설명을 제공한다.

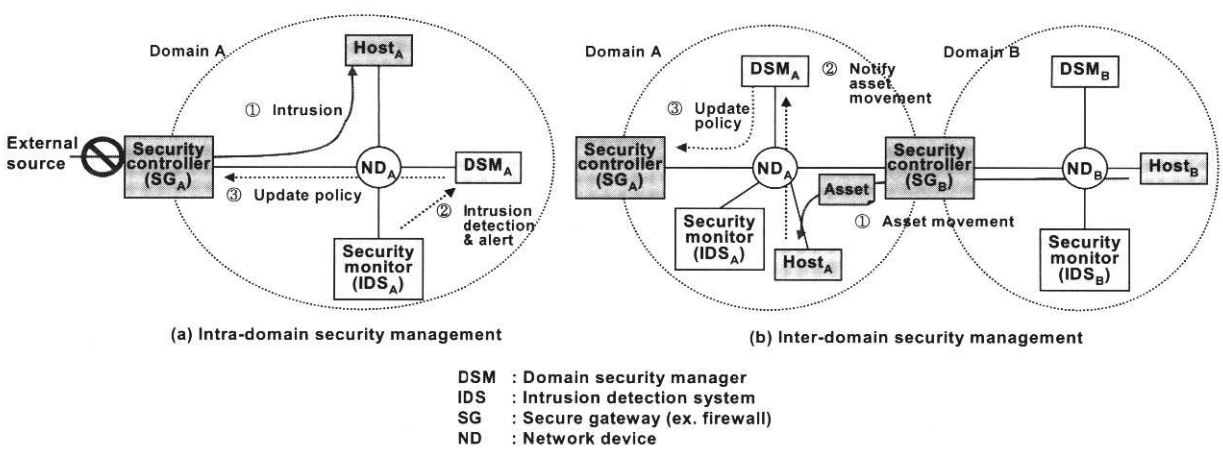
5.1 PRISM의 보안관리 유형

PRISM 모델에서의 보안 관리는 그 유형에 따라 사건대응 보안관리와 위험예방 보안관리의 두 가지로 분류된다. (그림 5)는 이 두 가지 유형의 보안관리를 도식화 한 것이다.

5.1.1 사건대응 보안관리

(그림 5)(a)는 외부에서의 침입이나 공격 징후가 발견되었을 경우 보안 감시자는 이를 DSM에 통지하고 DSM은 보안 제어자에게 관련된 통신을 차단하도록 정책을 전달함으로써 보안사건에 대한 자율적인 대응을 수행하는 절차를 나타낸다.

사건대응 보안관리는 발생한 보안 사건이나 정책의 대상의 상태에 따라 정책에 정의된 대응 행동을 수행하는 보안 관리이다. 여기서의 사건은 IDS에 정의된 공격 signature에 부



(그림 5) PRISM 모델의 보안관리

합된 내용이 발견되었을 경우, 취약성 점검 도구를 통해 취약성이 발견되었을 경우, 기타 보안 감시자에 의해 보안 관련 사건들이 발견되었을 경우이다.

감지된 사건에 대해서 PRISM은 기존의 통합보안관리가 제공하는 자동적인 대응 행위를 수행한다. 즉, IDS에 대해서는 역추적, 세션 강제 종료, 방화벽에서의 접근 거부, 취약성 제거를 위한 소프트웨어 갱신(update), 패치(patch), 설정 변경(configuration) 등의 행위가 대응 행위가 된다.

사건대응 보안관리 규칙은 사건대응 보안관리 정책에 의해 정의된다.

5.1.2 위험예방 보안관리

(그림 5)(b)는 자산의 이동을 감지한 호스트나 보안 감시자는 이 사실을 DSM에게 통지하고 DSM은 해당 자산의 보호를 위해 보안 제어자에게 해당 자산을 저장하고 있는 호스트로의 접근을 제어하도록 정책을 전달한다. PRISM은 이러한 과정을 통해 중요 자산에 대해 보안사고 예방 차원의 보안관리를 수행한다.

위험예방 보안관리는 자산 이동, 복제나 자산 상태 변화에 대해 보안 위협들로부터 자산을 보호하기 위해 정의된 정책을 통해 수행되는 보안 관리이다.

PRISM 모델에서 자산의 이동/복제/상태변화를 감지한 DSM은 자산의 중요도와 현재 자산이 위치한 곳의 보안성을 비교하여 위험예방 보안관리 정책에 정의된 규칙에 따라 해당 자산이 다루어지는 지점에 대한 보안성을 높이거나 감시를 강화하는 등의 대응 행위를 취한다.

위험예방 보안관리 규칙은 위험예방 보안관리 정책에 의해 정의된다.

이와 같이 두 가지 유형의 보안관리는 보안 사건 발생 이전에 자산을 보호하는 보안관리 뿐만 아니라 보안 사건 발생 후에 이에 대응하는 사후 대응 방식의 이중적인 보안관리 활동이 가능하게 함으로써 강도 높은 보안관리를 제공한다.

PRISM의 보안 관리 유형이 두 가지로 분류됨에 따라 PRISM의 보안 관리 정책 역시 각각의 보안 관리 유형에 따라 두 가지로 정의된다. 즉, 사건대응 보안관리 정책과 위험예방 보안관리 정책의 두 가지 보안관리 정책이 정의된다.

5.2 보안 레이블

PRISM에서 보안 정책의 인자로 사용되는 보안 레이블은 도메인과 호스트의 보안 수준을 나타내는 보안 수준과 자산의 중요도를 나타내는 중요도의 두 가지가 정의되어 있다.

정책은 어떠한 조건에 대한 행위를 결정하는 규칙이므로 정책은 최소한 '조건(condition)'과 '행위(action)'로 구성된다. 위험예방 보안관리 정책에서의 '조건'은 도메인과 호스트의 보안수준 그리고 자산의 중요도를 주요 인자로 사용한다. 따라서, 통합보안관리 정책을 위해 도메인과 호스트의 보안 수준의 사전 평가와 보안수준을 결정하는 기준이 필요하다.

PRISM에서는 자산의 이동에 대한 위험도를 평가하여 예방 조치를 취하기 위해 이 평가 지표로써 관리 대상 객체들에 부여된 보안 레이블을 이용한다. 보안 레이블이 부여되는 관리 객체는 자산과 호스트/도메인 객체이다. 보안 레이블은 자산의 중요도(sensitivity level)와 호스트/도메인의 보안 수준(security level)의 두 가지가 존재한다.

PRISM 모델에서 보안 수준과 자산 중요도는 very high(+2), high(+1), medium(0), low(-1), very low(-2)의 다섯 가지 등급으로 나눈다. 이 등급을 나누는 기준은 기존의 자산 평가 및 위험분석 기술의 적용 결과를 따를 수 있으며, PRISM에서는 현재 이 보안 레이블의 결정은 조직의 보안 정책에 입각하여 보안관리자가 판단하여 부여하는 것으로 하며 그 기준은 <표 3>에 나타나 있다.

〈표 3〉 보안 레이블

Grade	Security labels	
	Security level (for domain & host)	Sensitivity level (for asset)
Very high (+2)	조직의 문서화된 보안 정책에 따라 물리적 보안을 포함한 보안 대책이 갖추어진 경우 보안사고에 대한 대응 절차가 문서화 되어 시행되고 있는 경우 (문서화된 보안정책, 보안대책, 사고대응 절차, 정기적인 감시 활동)	파괴, 변조, 유출 되었을 경우 조직의 장기적인 업무 마비를 초래할 수 있는 자산 (장기적인 업무 마비, 자산 복구 불가)
High (+1)	알려진 취약성에 대해 보안 대책이 취해져 있으며 조직의 보안 정책에 따라 감시활동이 이루어지고 있는 경우 (문서화된 보안정책, 보안대책, 정기적인 감시 활동)	파괴, 변조, 유출 되었을 경우 일시적인 업무 마비를 초래할 수 있는 자산 (단기적인 업무 마비, 자산 복구 가능)
Medium (0)	알려진 취약성에 대해 적절한 대책이 취해져 있는 경우 (보안대책, 정기적인 감시)	파괴, 변조, 유출 되었을 경우 조직의 업무 수행에 일시적인 불편을 초래할 수 있는 경우 (일시적 업무 마비, 자산 복구 가능)
Low (-1)	알려진 취약성에 대한 대책이 완전하지는 않으나 부정기적인 보안 점검이 이루어지고 있는 경우 (보안대책, 부정기적인 감시)	파괴, 변조, 유출 되었을 경우 조직의 업무에 거의 영향이 없는 경우 (자산 복구 가능)
Very low (-2)	보안 대책이 전무한 경우	파괴, 변조, 유출 되었을 경우 조직의 업무에 영향이 없는 경우 (자산 복구 불필요)

참고로, PRISM에서 사용하는 보안 레이블 결정의 기준은 자산 및 위험평가 절차에서 제시된 포괄적인 기준을 참고로 하여 결정한 지표이다.

6. PRISM의 동작 절차와 평가

본 장에서는 PRISM의 핵심 개념인 위험예방 동작 절차를 설명하고 기존 통합보안관리 방식과 PRISM의 비교 및 PRISM의 잠재적인 문제점을 진단한다.

6.1 PRISM의 위험예방 동작 절차

본 장에서는 PRISM 모델의 관리 대상 네트워크 상의 두 도메인 간에 자산 이동이 발생할 경우의 예를 들어 위험예방 보안관리가 어떠한 절차에 따라 이루어지는지를 소개한다.

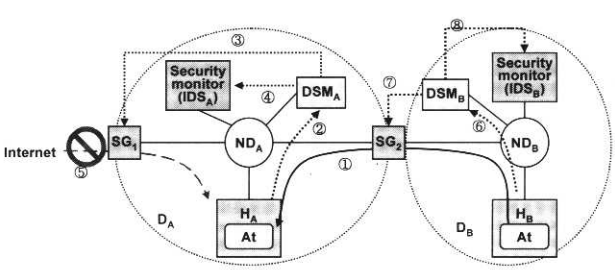
(그림 6)의 의사코드는 PRISM 모델에서 자산의 변화를 감지한 이후의 처리과정을 나타내고 있다. 자산 상태 변화 사건이 감지되면 이를 일단 자산정보 추적 DB에 기록한다(line 14). 자산의 변화에 따른 처리는 위험예방 보안관리가 수행되므로 위험예방 보안정책을 조회한다(line 15). 다음으로, 자산의 중요도와 자산이 현재 위치한 호스트/도메인의 보안 수준을 비교하여 다음으로 수행되어야 할 행위가 결정된다. 이 때, 위험예방 보안정책이 단일 호스트를 대상으로 하는 경우와 도메인을 대상으로 하는 경우로 나뉘며, 이는 보안관리자가 사전에 위험예방 보안정책을 어떤 범위로 설정하느냐 하는 데에 달려있다. 보안관리 영역이 협소한 경우, 도메인 단위로 위험예방 보안정책을 적용하는 것이 직접 관련된 호스트 외의 타 호스트로의 위험의 확산을 사전에 방지할 수 있으며, 보안성을 높이는 데 도움이 된다. 그러나, 보안관리 대상 도메인 내에 다수의 호스트가 존재하는 경우, 도메인 전체에 대한 보안정책 적용은 각각의 호스트에 대한 정책 설정, 다수 보안시스템에 대한 정책 전달 등의 보안관리 과정에 시간과 자원을 많이 소요하므로 이 경우는 직접 관련이 있는 호스트로 보안정책 적용 범위를 제한 하는 것이 관리의 효율성을 기대할 수 있다. 따라서, 위험예방 보안정책에 설정된 적용 범위가 호스트인 경우(line 17)와 보안정책 적용 범위가 도메인인 경우(line 24)로 나뉘어 이후의 처리과정이 진행된다. 각각의 경우 보안정책 적용 범위의 차이가 있을 뿐, 처리 과정은 유사하다. 자산의 중요도가 자산이 현재 위치한 호스트/도메인의 보안수준보다 높은 경우(line 18, line 25)는 도메인 내의 보안시스템의 보안 정책을 변경하는 절차가 수행된다. 즉, 방화벽의 접근제어 정책을 통해 해당 호스트/도메인으로의 접근을 제한하고(line 19, line 26), IDS의 보안감시를 강화하며(line 20, line 27), 자산이 위치한 호스트에 존재하는 보안 취약성을 점검한다(line 21, line 28). 자산의 중요도보다 호스트/도메인의 보안 수준이 높은 경우 즉, 보안 상태가 양호한 경우 다른 절차가 수행될 필요는 없다(line 23, line 30). 마지막으로, 위험예방 보안관리 절차가 종료되면, 이에 대한 기록을 로그 정보로 남긴다(line 33).

```
1  : int fwPolicySet(src, dst, rule) ;
2  : int idsPolicySet(object, rule) ;
3  : hostVulnerabilityCheck(object) ;
4  :
5  : class asset {
6  : int id ;
7  : char* name ;
8  : int sensLevel ;   # -2 to 2
9  : host currentHost ;
10 : domain currentDomain ;
11 : char* description ;
12 : }
13 :
14 : updateAssetDB(asset) ; # save current asset information
15 : preventivePolicy = getPreventivePolicy(asset) ;
16 :
17 : if (preventivePolicy.objectScope = HOST_SCOPE) {
18 :   if (asset.senLevel > asset.currentHost.secLevel) {
19 :     fwPolicySet(any, asset.currentHost, deny) ;
20 :     idsPolicySet(asset.currentHost, monitor) ;
21 :     hostVulnerabilityCheck(asset.currentHost) ;
22 :   } else { # asset.senLevel ≤ host.secLevel
23 :     doNothing() ;
24 : } else { # preventivePolicy.objectScope = DOMAIN_SCOPE
25 :   if (asset.senLevel > asset.currentDomain.secLevel) {
26 :     fwPolicySet(any, asset.currentDomain, deny) ;
27 :     idsPolicySet(asset.currentDomain, monitor) ;
28 :     hostVulnerabilityCheck(asset.currentDomain) ;
29 :   } else { # (asset.senLevel ≤ domain.secLevel)
30 :     doNothing() ;
31 : }
32 :   .
33 : logEvent() ;
```

(그림 6) PRISM의 자산변화 대응 의사코드

위험예방 보안관리의 수행 과정을 예가 (그림 7)에 나타나 있으며, 이를 설명하면 다음과 같다.

관리 대상 네트워크는 두 도메인 D_A, D_B로 구성되며, 각각 그 내부에 호스트 H_A, H_B, 보안 감시자 IDS_A, IDS_B, 네트워크 장치 ND_A, ND_B가 있다. 이들 두 도메인 사이에는 보안 제어자인 보안게이트웨이 SG_2가 있고 도메인 D_A와 외부 네트워크인 인터넷 사이에는 보안게이트웨이 SG_1이 존재한다.



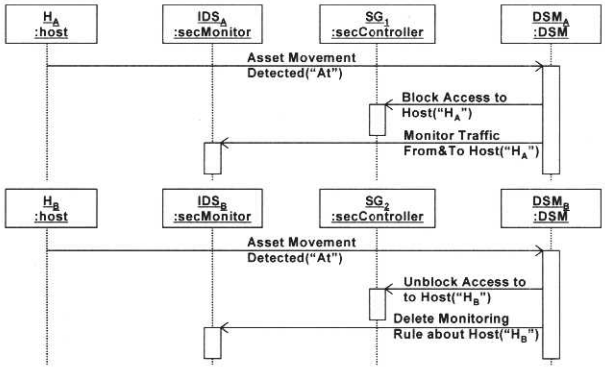
(그림 7) 위험예방 보안관리 동작

가정 1) 자산 이동 이전에 보안 감시자 IDS_B와 보안 제어자 SG_2는 각각 최초 At를 보유한 H_B에 대해 각각 감시 정책과 접근제어 정책이 설정되어 있다.

가정 2) 자산 At의 중요도와 H_A의 보안성 비교 결과 H_A의 보안성은 At의 중요도 보다 낮으므로 충분한 보안성을 확보하지 못한 상태이다.

① 자산 At가 호스트 H_B에서 H_A로 이동한다. 이 때 자산의 이동이므로, At의 원본은 H_B에서 삭제된다.
② 관리 대상 호스트 H_A는 자신이 속한 도메인의 DSM_A에게 자산 이동을 보고한다.
③ DSM_A는 At의 중요도보다 H_A의 보안성이 낮음을 감지하고 호스트 H_A에 보안 감시를 강화하도록 IDS_A의 감시 정책을 갱신한다.
④ DSM_A는 추가적으로 호스트 H_A에 대한 외부에서의 접근을 차단하도록 SG_1의 접근제어 정책을 갱신한다.
⑤ 위험예방 보안관리 절차의 처리 결과로 외부에서 H_A로의 접근은 사전에 차단된다.

도메인 D_A에서 일어나는 위험예방 보안관리 절차에 이어서 자산이 원래 위치해 있던 도메인 D_B에서의 보안관리 절차는 다음과 같다. 이 후속조치는 보안자원의 절감을 위해 보안관리의 효율성 향상을 목적으로 한다.



(그림 8) 위험예방 보안관리 순서도

⑥ 호스트 H_B는 자산 At의 이동 후 원본이 삭제되어 더이상 자신에게 자산 At가 존재하지 않음을 알린다.
⑦ DSM_B는 자산 파기를 알려온 시스템에 대한 보안 상태와 자산 보유 현황을 재 평가하여 해당 시스템에 대한 보안 감시 및 보안제어 정책이 필요 없다고 판단하면, SG_2 상의 이전에 At의 보유로 인해 설정된 H_B에 대한 접근제한 정책을 제거한다.
⑧ DSM_B는 보안 감시자에 대해서도 H_B에 대한 보안감시 정책을 제거한다.

(그림 8)은 이러한 처리 과정을 관련된 객체와 이들 사이에 전달되는 메시지를 명시하여 순서도로 표현한 것이다.

6.2 기존 통합보안관리와 PRISM의 비교

기존의 사후대응 방식의 보안관리와 비교하여 PRISM의 장점을 요약하면 다음과 같다.

① 자산의 중요도를 고려한 보안자원의 효율적 분배

기존의 보안관리는 호스트와 네트워크를 주요 관리 대상으로 하여 관리영역 내의 각 호스트들이나 네트워크들에 대해 거의 동일한 보안정책을 수립하여 포괄적인 보안관리를 수행하였다. 그러나, 실세계의 업무 네트워크에서는 호스트나 네트워크의 중요도와 이들이 처리하는 자산의 중요성이 각기 다르다. 이와 같이, 차별적인 보안요구를 무시하고 각 대상에 대해 동일한 보안자원/정책을 적용하는 것은 보안자원과 정책의 부적절한 배분을 초래한다.

일반적으로 보안성과 서비스 품질 및 서비스 이용 편의성은 반비례 관계이다. 이러한 관계를 고려하지 않고 동일한 보안자원/정책을 적용하여 보안성을 높이려 함은 실제로 보안이 크게 필요하지 않음에도 사용자의 편이성과 서비스 품질을 저하시키는 결과를 낳기도 한다.

PRISM에서는 사전에 정의된, 자산이 요구하는 보안수준에 따라 각 호스트/도메인에 대해 차별적인 보안자원을 할당함으로써 서비스들에 대한 성능 영향을 필요한 수준 정도로 감소시키며, 각 보안 시스템들에게 필수적인 보안 정책만을 적용하여 이들이 보안정책의 수에 따른 부담을 감소시키고 보안시스템의 성능 향상을 도모한다.

② 자산 상태 감시를 바탕으로 한 자율적 사전 대응 방식의 보안관리

기존의 통합보안관리 기술은 감지된 보안사건에 자율적으로 대응하는 방식의 사후 대응방식으로써 수동적인 보안관리 기술이다. 보안관리 대상 영역에 다수의 호스트/도메인이 존재하는 경우, 보안관리자가 이들에 대해 모든 보안정책을 수립하고 적용하는 것은 많은 노력과 시간이 요구되는 작업일 뿐만 아니라, 유동적으로 변화하는 자산의 중요도에 대해 적절한 보안성을 지속적으로 제공하기가 어렵다.

PRISM에서는 자산의 상태 변화를 주요 감시 대상으로 하여 자산이 위치하는 호스트/도메인에 대해 사전에 능동적으로 보안 점검을 수행하고 보안 시스템들을 이용한 접근제어, 인증, 감시 등을 강화하여 공격자에 의한 공격 성공 확률을 감소시킬 수 있다.

③ 위험예방과 사후 대응의 2중 보안 대책을 통한 높은 보안성을 제공

기존의 통합보안관리 방식은 보안사건의 감지와 자율적인 대응을 주목표로 개발되어 왔다. 즉, 침입자의 침입을 감시하고 발생한 보안사건에 대해서 보안 시스템들의 대응 행위를 지시하여 공격의 진행이나 피해의 확산을 막기 위한 보안관리 기술이다. 그러나, 이 과정에서 공격이 이미 어느 정도 진행되었을 수도 있고 사후 대응 방식으로는 날로 변화되어가는 공격기술에 대해 적절히 대응하기가 힘든 것이 사실이다.

PRISM은 사전예방 보안관리와 사후대응 보안관리의 2중

보안관리를 수행하여 자산에 대한 보안 위험을 감소시킨다. 즉, 자산의 추적을 통해 자산 상태의 변화에 따라 자율적으로 보안 예방대책을 마련하여 공격성공 가능성을 감소시키고, 보안사건 감지 이후는 기존 통합보안관리 방식의 자율적인 대응을 통한 보안관리를 수행하여 보안성을 높인다.

한편, 잠재적으로 예상되는 PRISM의 문제점은 다음과 같다.

① 대량의 자산 정보 관리의 어려움

실제 호스트/도메인의 수 보다 이들 내에서 처리하는 자산의 종류와 수는 비교할 수 없을 만큼 방대하다. PRISM은 자산 상태 추적을 기반으로 하고 있는 이유로 이들 관리 대상 영역내의 주요 자산들에 대한 정보를 관리하는 것은 많은 자원을 요구한다. 따라서, 효율적인 정보 관리 구조와 관리 대상 자산 범위의 제한 등의 규칙에 대한 연구를 통해 이를 해소하여야 한다.

② 호스트에 대한 사전 취약성 점검의 지연

자산이 이동해가거나 복사되어간 호스트가 보안수준이 낮은 경우 이 호스트가 요구되는 보안수준을 성취하기 위해서 호스트에 대한 취약성 점검이 수행되어야 한다. 그러나, 취약성 점검은 해당 호스트의 자원을 점유하며 취약성 점검이 종료되기까지 시간 지연이 존재한다. 결과적으로, 호스트에서 이루어지는 서비스의 품질에 영향을 줄 소지가 있으며, 취약성 점검이 완전히 종료되어 그 대책이 적용되기 까지 해당 호스트 상의 자산은 안전하지 못한 상태로 있게 된다. 사용자가 서비스 이용에 불편을 느끼지 못하도록 취약성 점검 기술의 효율성을 높이고 취약성 점검 및 대책 적용에 존재하는 지연을 최소화하는 방법에 대한 연구가 필요하다.

7. 결론 및 향후 계획

현재의 사이버 범죄는 점점 지능화, 복잡화 되고 있으며, 지금도 새로운 공격 방법이 끊임없이 나타나고 있다. 기존의 사후대응 방식의 통합보안 관리는 대응 조치가 취해지기 전 까지는 공격에 의한 피해 가능성이 존재하며, 공격자가 유용한 정보를 취할 수도 있다. 한편, 자산의 중요도를 무시한 보안 정책으로는 필요 이상 과도한 대응 비용을 소비하기도 한다.

본 논문에서는 사후대응 방식의 통합보안관리의 단점을 극복하고자 사전에 위험을 예방하는 방식의 통합보안관리 모델인 PRISM을 제시하였다. PRISM은 사전 예방 방식의 보안관리 과정에서 각 자산의 중요도를 할당하고 그에 따라 적절한 수준의 대응을 함으로써 각 보안 시스템의 과도한 자원 낭비나 대응 비용의 낭비를 막을 수 있다.

PRISM 모델의 구체적인 실현을 위해서 가장 중요한 것은 앞으로 위험분석 모델의 연구와 정제를 통해 자산 가치 평가/정량화 방법이 제시되어야 하며, 이와 함께 호스트와 도메인의 보안 수준 평가/정량화 방법론에 대한 연구도 필요하다. 또한 각 관리 객체 정보의 구조 설계, 정책 전파 프로토콜의 설계가 이루어져야 한다.

PRISM 모델에서 잠재적으로 예상되는 문제점은 네트워크에 산재해 있는 방대한 자산 정보의 추적과 관리가 그리 쉽지 않다는 것을 들 수 있다. 따라서, 앞으로 대규모 네트워크 상의 방대한 자산 정보의 관리를 위한 효율적인 정보 관리 구조의 연구가 필요하며, 현재는 각 도메인 내에서 자산정보를 관리하는 분산 방식에 대한 모델을 고려중이다.

참 고 문 헌

[1] Dorothy E. Denning, "Information Warfare and Security," ACM Press, 1999.

[2] Rebecca G. Bace, "Intrusion Detection," Macmillan Technical Publishing, 2000.

[3] David J. Marchette, "Computer Intrusion Detection and Network Monitoring : A Statistical Viewpoint," Springer-Verlag, 2001.

[4] William R. Cheswick, Steven M. Bellovin, "Firewalls and Internet Security-repelling the wily hacker," Addison Wesley, 1994.

[5] Robert L. Ziegler, "Linux Firewalls," New Riders Publishing, 2000.

[6] Matt Bishop, "Computer Security : Art and Science," Pearson Education, 2003.

[7] Charles P. Pfleeger and Shari Lawrence Pfleeger, "Security in Computing," 3rd ed., Pearson Education, 2003.

[8] "Secure Virtual Network Architecture : A Customer-focused White Paper," Check Point Software Technologies Ltd., Nov., 2000.

[9] "Open Platform for Security(OPSEC) Technical Note," Check Point Software Technology, Inc., 2000.

[10] Dan Schnackengerg, Kelly Djahandari, Dan Sterne, "Infrastructure for intrusion detection and response," DARPA Information Survivability Conference and Exposition 2000, DISXCE '00 Proceedings, Vol.2, pp.25-27, Jan., 2000.

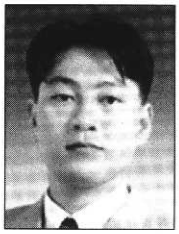
[11] Dan Schnackengerg, Harley Holliday, Randall Smith, Kelly Djahandari, Dan Sterne, "Cooperative Intrusion Traceback and Response Architecture (CITRA)," DARPA Information Survivability Conference & Exposition II, DISXCE '01 Proceedings, Vol.1, pp.56-68, Jun., 2001.

[12] D. Y. Lee, D. S. Kim, K. H. Pang, H. S. Kim, T. M. Chung, "A Design of Scalable SNMP Agent for Managing Heterogeneous Security Systems," NOMS 2000, Apr., 2000.

[13] 김동수, 정태명, "중앙 정책 데이터베이스를 이용한 방화벽 통합 관리 시스템 개발", 제13회 한국정보처리학회 춘계학술대회, Apr., 2000.

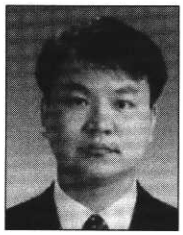
[14] 이동영, 김동수, 홍승선, 정태명, "웹 기반의 방화벽 통합 보안관리 시스템 개발", 정보처리학회논문지, 제7권 제10호, pp. 3171-3181, Oct., 2000.

[15] 이동영, 김동수, 정태명, "이종의 보안시스템 관리를 위한 정책 기반의 통합보안관리시스템의 정책모델에 관한 연구", 정보처리학회논문지C, 제8-C권 제 5호, pp.565-572, Oct., 2001.



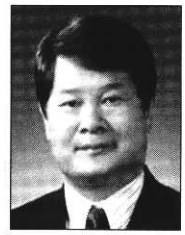
김 동 수

e-mail : dskim@imtl.skku.ac.kr
1998년 성균관대학교 정보공학과(학사)
2000년 성균관대학교 일반대학원 전기전자 및 컴퓨터공학과(석사)
2000년~현재 성균관대학교 정보통신공학부 컴퓨터공학전공 박사과정 재학
관심분야 : 통합보안관리, 무선인터넷 보안, 서비스 관리



김 태 경

e-mail : tkkim@imtl.skku.ac.kr
1997년 단국대학교 수학교육과(학사)
2001년 성균관대학교 정보통신대학원 정보통신공학과(석사)
2001년~현재 성균관대학교 정보통신공학부 컴퓨터공학전공 박사과정 재학
관심분야 : 침입탐지 시스템, GRID 컴퓨팅, 서비스 관리



정 태 명

e-mail : tmchung@ece.skku.ac.kr
1981년 연세대학교 전기공학과(학사)
1984년 University of Illinois Chicago, 전자계산학과(학사)
1987년 University of Illinois Chicago, 컴퓨터 공학과(석사)
1995년 Purdue University, 컴퓨터 공학과(박사)
1985년~1987년 Waldner and Co., Systems Engineer.
1987년~1990년 Bolt Bernek and Newman Labs., Staff Scientist
1995년~현재 성균관대학교 정보통신공학부 교수
관심분야 : 실시간 시스템, 네트워크 관리, 통합보안관리