대규모 네트워크 환경에서의 보안관리를 위한 보안평가 시스템 설계

(Design of the Security Evaluation System for Decision Support in the Enterprise Network Security Management)

이 재 승 † 김 상 춘 ††
(Jae Seung Lee) (Sang Choon Kim)

요 약 보안평가 시스템은 다양한 요소로 구성된 대규모 네트워크 도메인 전체의 보안성을 평가하고 이를 바탕으로 보안 관리자 혹은 보안관리 시스템이 네트워크 보안관리를 수행하는데 필요한 의사결정을 지원하는 시스템이다. 이 시스템은 보안상 취약점들로 인한 공격을 방지하기 위해 어떻게 네트워크의 보안 관련 설정을 해주어야 하는지에 관한 의사결정을 지원해 준다. 보안평가 시스템은 네트워크의 "현재 상태"를 분석하고 공격 가능성을 찾아내어 불법적인 침해 행위를 사전에 예방하도록 보안관리의 의사결정을 지원해 준다. 본 논문에서는 다양한 요소로 구성된 대규모 네트워크의 보안성 평가를 자동화하고 침해사고 예방을 위해 보안관리의 의사결정을 도와주는 보안평가 시스템에 대한 요구 사항을 분석하고 이를 반영한 보안평가 시스템을 설계한다.

키워드 : 보안평가 시스템, 네트워크 보안관리

Abstract Security Evaluation System is a system that evaluates the security of the entire enterprise network domain which consists of various components and that supports a security manager or a Security Management System in making decisions about security management of the enterprise network based on the evaluation. It helps the security manager or the security management system to make a decision about how to change the configuration of the network to prevent the attack due to the security vulnerabilities of the network. Security Evaluation System checks the "current status" of the network, predicts the possible intrusion and supports decision-making about security management to prevent the intrusion in advance. In this paper we analyze the requirements of the Security Evaluation System that automates the security evaluation of the enterprise network which consists of various components and that supports decision-making about security management to prevent the intrusion, and we propose a design for it which satisfies the requirements.

Key words : Security Evaluation System, Network Security Management

1. 서 론

1.1 보안평가 시스템 개요

네트워크 사용의 급격한 증가로 최근에는 특정 호스트의 보안 문제뿐만 아니라 많은 구성요소를 포함하고 있는 대규모 네트워크 전체의 보안 문제가 더욱 중요해졌다. 대규모 네트워크의 보안 상태를 일정 수준 이상으로 유지하기 위해서는 방화벽[1]이나 침입 탐지 시스템[2] 이외에도 시스템 및 네트워크의 현재 상태를 분석하여 보안성을 평가하고 여기에서 발견된 보안상 문제점들로 인해 발생 가능한 불법적인 침입을 예방하도록 보안관리의 의사결정을 지원해주는 시스템이 필요하다.

보안평가를 위해서는 많은 종류의 보안성 시험과 분석이 필요하며 대규모의 네트워크 환경에서 이를 몇몇 보안 관리자가 수행하기는 매우 어렵기 때문에 이러한 시험과 분석을 자동으로 수행해 주는 도구가 필요하다. 이러한 도구는 특정 호스트 혹은 서브 네트워크의 보안상 취약점뿐만 아니라 이들을 종합한 대규모 네트워크 도메인 전체의 보안성을 분석해 내고 보안상 문제점을 해결할 수 있도록 보안관리에 필요한 의사결정을 지원해 줄 수 있어야 한다.

† 정 회 원 : 한국전자통신연구원 정보보호연구본부 연구원
jasonlee@etri.re.kr
†† 비 회 원 : 삼척대학교 정보통신공학과 교수
kimsc@samcheok.ac.kr
논문접수 : 2003년 5월 15일
심사완료 : 2003년 8월 22일

보안평가 시스템은 네트워크 혹은 시스템 구성 요소의 보안상 취약점 및 잘못된 설정을 자동화된 도구로 분석하여 특정 호스트 및 서브 네트워크별 보안성뿐만 아니라 네트워크 도메인 전체의 보안성을 평가해주고 보안상 문제점으로 인한 공격을 사전에 막을 수 있도록 보안관리에 관한 의사 결정을 지원해 주는 시스템이다. 이 시스템은 침입 탐지 시스템[2]처럼 공격이 발생한 시점에서 침입 사실을 탐지하여 이를 막기보다는 시스템의 "현재 상태"를 분석하여 네트워크의 보안성을 평가하고 발생 가능한 공격에 대처할 수 있도록 보안관리의 의사결정을 지원하여 침입이 일어나기 전에 이를 예방하도록 도와준다.

1.2 보안평가 시스템 연구의 필요성

보안평가 시스템을 위한 정형화되고 표준화된 기술은 아직 없으며, 개별 업체들이 독자적 형태로 개발한 호스트 및 네트워크 취약성 분석 툴을 사용하여 보안평가에 활용하고 있는 실정이다.

COPS[3], SATAN[4], Nessus[5] 등의 해킹 툴을 사용하여 시스템 및 네트워크의 취약점을 분석하여 보안평가에 활용하는 방법이 널리 사용되고 있으나 개별 툴들이 통합되지 않았고 각 툴에서 발견된 보안 취약점들을 통합 분석한 종합적인 분석결과를 얻어내기 어렵고, 새로운 취약점이 나올 때마다 개별 툴을 일일이 업데이트 해야 하는 단점이 있으며 대부분 네트워크를 스캐닝하여 몇 가지 알려진 보안상 취약점에 대한 보고를 해주는 정도의 기능만을 제공해 주고 있다.

Symantec의 NetRecon[6], ISS[7]의 Internet Scanner, System Scanner, Symantec의 Vulnerability Assessment[6] 등의 상용 취약성 분석 툴을 보안평가에 활용하기도 하나 이들 툴도 시스템 혹은 네트워크의 취약점을 스캐닝 해주는 기능을 제공해 주는 정도이다.

보안평가 시스템은 앞으로 자동화된 새로운 취약점에 대한 검색 기능 업데이트, 해킹 시뮬레이션을 이용한 취약점 분석, 보안 정책 서버와의 연동, 보안 관리 서버와 연동한 취약점 복구, 특정 취약점으로 인한 침입 가능성 분석, 전체 시스템 보안 수준 향상을 위한 조언 기능, 대규모 네트워크 환경을 위한 확장성 등을 제공하는 방향으로 발전하여야 하나 아직 이에 대한 연구가 불충분하고 이러한 기술을 모두 구현하고 있는 툴은 거의 없는 실정이다. 따라서 보안평가 시스템에 대한 보다 심화된 연구와 개발이 필요하다.

이 논문에서는 시스템 및 네트워크의 보안평가 방법 및 취약성 분석 도구에 대해 분석하고 보안평가 시스템에 대한 요구 사항을 도출하며 이를 수용한 보안평가 시스템을 설계한다.

2. 보안평가 방법

이 절에서는 시스템 및 네트워크의 보안성을 평가하기 위한 보안평가 방법에 대해 알아본다.

2.1 보안평가 방법 개요

많은 침해 사고는 운영체제 및 소프트웨어의 버그, 잘못된 시스템 설정, 관리상의 실수로 인한 경우가 많으며 이러한 보안상 문제점을 찾아내고 분석한 결과가 보안평가의 중요한 자료가 된다. 보안평가의 종류는 독립형 시스템에 대한 보안평가와 네트워크에 연결된 시스템에 대한 보안평가의 두 가지로 나누어 볼 수 있다.

독립형 시스템에 대한 보안평가의 경우 시스템 사용자간 공유되는 파일 및 디렉토리의 권한 설정, 패스워드 길이, 시스템 구성 등이 올바르게 설정되어 있는지를 조사한다. 특히 시스템의 설정과 직접적으로 연관되어 있는 시스템 파일, 운영체제 및 주요 소프트웨어의 버그 패치 상황 등을 집중적으로 분석하게 된다.

네트워크에 연결되어 있는 시스템의 경우 다수 시스템 간의 자원 공유 및 네트워크 서비스의 보안상 취약점 등으로 인하여 불법적인 접근에 대한 문제가 더욱 복잡해진다. 다른 사용자 혹은 시스템으로 위장하여 접근을 하거나 트로이 목마 설치, 네트워크 서비스의 보안상 허점을 이용한 원격지에서의 공격 등의 문제가 발생할 수 있으며 이를 사전에 막기 위해 네트워크 관련 시스템 파일 및 네트워크 서비스 설정, 운영체제 버그 패치 상황 등을 분석하게 된다[8].

2.2 보안성 분석 기법

보안성 분석을 위해 해킹 시뮬레이션 등을 통해 시스템에 직접 침입을 시도해 보거나 단순히 시스템을 관찰하여 시스템의 상태를 분석함으로써 보안상의 문제점을 찾을 수도 있다. 네트워크 환경 하에서는 네트워크 링크를 경유하여 원격지의 시스템에서 제공하는 네트워크 서비스의 보안성을 분석해 볼 수 있고 분산 환경 하에서의 각 호스트의 역할에 따라 관련된 각 호스트들을 분석하여 보안성을 분석해 볼 수도 있다.

시스템 설정 파일들을 분석하여 구성상의 오류를 점검해 보아야 하며 시스템 명령어 파일들과 시스템 유틸리티들의 사용 권한을 확인해 보아야 한다. 또한 운영체제나 시스템 프로그램의 버그 패치가 제대로 설치되어 있는지 확인해 보아야 하고 중요한 시스템 파일에 대해서는 파일의 무결성을 확인해 보아야 한다.

특정 보안상 허점으로 인해 발생 가능한 연쇄적인 보안상 문제점이나 공격 시나리오를 예측하는 것은 어려우며 이것을 알아내기 위해서는 일정한 규칙을 설정하고 이를 특정 보안상 허점과 매치시켜 볼 수 있어야 한다. 이러한 작업에는 규칙기반(rule-based) 인공지능 기법 사용이 적합하다[9].

3. 취약점 분석 도구

보안평가의 기초가 되는 것은 많은 종류의 보안성 시험과 분석을 통해 얻은 시스템 및 네트워크의 취약점에 대한 데이타이며 대규모의 네트워크 환경에서 이러한 시험과 분석을 몇몇 관리자가 일일이 수행하기는 어렵기 때문에 이를 자동으로 수행해 주는 도구가 필요하다. 이러한 취약점분석 도구는 크게 네트워크 스캐너(Network-based scanner)와 호스트 스캐너(Host-based scanner)로 나뉘어 진다[10].

네트워크 스캐너는 전체 네트워크 구성 요소들의 취약점을 한곳에서 전체적으로 파악할 수 있도록 해주며 호스트 스캐너는 각 호스트의 하위 레벨의 세세한 사항까지 직접 액세스하여 점검할 수 있도록 해주어 중요한 서버들의 보안상 취약점을 보다 세밀하게 조사하는데 적합하다. 보안상 위협을 철저히 분석하기 위해서는 두 가지 종류의 스캐너를 모두 사용하는 것이 좋다.

3.1 네트워크 스캐너(Network-based Scanner)

네트워크 스캐너는 네트워크 구성 요소들의 보안상 취약점을 조사하며 네트워크를 통해 시스템에 침입하려는 외부 혹은 내부의 침입자의 입장에서 조직 전체의 네트워크 및 시스템을 자세하게 분석한다. 네트워크 스캐너의 특징은 다음과 같다[10].

- 네트워크 구성 요소들을 분석하고 자세한 보고서를 생성하여 보안상 취약점을 수정할 수 있도록 도와준다.
- 취약점을 조사할 각 호스트에 일일이 설치될 필요가 없기 때문에 설치 및 사용이 용이하다.
- 침입자가 네트워크를 통해 원격지의 시스템에 침입하는 기법을 사용해 네트워크의 취약점을 평가한다.
- 취약한 네트워크 서비스 등 네트워크 관련 취약점을 효율적으로 조사할 수 있다.

3.2 호스트 스캐너(Host-based Scanner)

호스트 스캐너는 호스트의 운영체제 및 특정 서비스, 시스템 설정 등에 대해 하위 레벨의 세세한 사항까지 직접 액세스 할 수 있다. 네트워크 스캐너는 네트워크를 통한 침입자의 관점에서 시스템의 보안상태를 분석하지만, 호스트 스캐너는 특정 호스트에 로컬 계정을 가지고 있는 사용자의 관점에서 시스템의 보안 상태를 분석한다. 호스트 스캐너의 특징은 다음과 같다[10,11].

- 보안에 위협이 되는 사용자의 보안 정책 위반 행위를 조사한다.
- 침입자가 시스템에 침투한 흔적을 찾아내며 중요한 파일에 변화가 있었는지를 검사한다.
- 스니퍼[4] 및 기타 허가받지 않은 서비스가 수행중인지 조사하여 침입자가 활동 중인지를 감지한다.
- Back Orifice와 같은 백도어 프로그램을 찾아내고 취약한 로컬 호스트 서비스들을 발견해 낸다.
- 취약한 패스워드 조사, 파일 시스템 점검 등을 네트워크 스캐너보다 효율적으로 수행한다.
- 중요한 서버들에 대해 일반적인 보안 점검 이외에 서버 설정 오류 등의 보다 자세한 보안 점검을 수행한다.

3.3 취약점 분석 도구 제품 현황

대표적인 취약점 분석 도구로는 COPS(Computerized Oracle and Password System)[3]와 SATAN (Security Administrator's Tool for Analyzing Networks)[12]이 있다.

COPS는 여러 개의 작은 프로그램들로 구성되어 있으며 각각의 프로그램들이 유닉스 시스템의 취약성 검사를 수행한다. 호스트 기반 취약성 검사 도구이며, 유닉스 환경에서만 사용할 수 있다.

SATAN은 취약성을 점검하고자 하는 대상 시스템에 모의 공격을 수행하여 취약성 여부를 판단한다. 네트워크 기반 취약성 검사 도구이기 때문에 네트워크를 통해 접근 불가능한 시스템 내부의 취약성은 점검할 수 없다.

현재 사용되고 있는 상용 취약점 분석 제품으로는 Symantec의 NetRecon[6], ISS[7]의 Internet Scanner, System Scanner, Symantec의 Vulnerability Assessment[6] 등이 있으며 시스템 혹은 네트워크의 취약점을 스캐닝 해주는 기능을 제공한다.

통합 환경 및 편리한 인터페이스를 제공하며 워크스테이션, PC뿐만 아니라 라우터 등의 통신장비까지도 분석해 주는 제품도 있으며 각 호스트 및 서브넷의 취약점을 종합 분석하여 이들에 대한 수정 방법을 제시해 주는 제품도 있다. 표 1은 주요 상용 취약점 분석 제품을 비교한 자료이다.

4. 보안평가 시스템 설계

이 절에서는 단순한 취약점 검색이 아닌 다양한 요소로 구성된 대규모 네트워크 전체의 보안평가를 수행하고 불법적인 침입을 미리 막을 수 있도록 보안관리에 필요한 의사결정을 지원하며 확장성을 갖는 보안평가 시스템에 대한 요구 사항을 분석하고 이를 반영한 보안평가 시스템을 설계한다.

4.1 보안평가 시스템에 대한 요구 사항

대규모 네트워크에서의 불법적인 공격을 막기 위한 보안평가 시스템에 대한 요구 사항은 다음과 같다.

- 다양한 요소로 구성된 대규모 네트워크 환경에서 사용 가능해야 하며 네트워크의 규모가 증가해도 처리 효율이 떨어지지 않도록 확장성을 가져야 한다.
- 보안평가 규칙을 이용하여 보안성 분석을 수행할 수 있어야 하고 규칙의 추가, 수정 등의 관리가 가능해야 한다[13].

표 1 상용 취약점 분석 제품 현황

제품	NetRecon	Internet Scanner	System Scanner	Vulnerability Assessment
회사	Symantec	ISS	ISS	Symantec
대상	네트워크 취약점 분석	네트워크 취약점 분석	시스템 취약점 분석	호스트 및 어플리케이션 취약점분석
특징	취약점에 대한 수정 방법 제시, 취약점 발견과정까지 설명	인트라넷, 방화벽, 웹 서버 검색 도구 통합	에이전트 이용, 시스템 수준의 취약점 분석	취약점에 대한 수정 방법 제시 라이브 업데이트 기술을 이용한 새로운 보안 모듈 업데이트 지원
운용 환경	Windows NT	Windows NT	UNIX, Windows 95/98/NT	Windows NT

- 시스템 설정 오류 검사, 해커 침입 흔적 추적, 트로이 목마 검색, 시스템 파일 무결성 점검 등 특정 호스트의 취약점 분석을 수행할 수 있어야 한다.
- 네트워크 서비스 취약점 분석을 비롯한 각 서브넷의 보안상 취약점 점검 및 분석을 수행할 수 있어야 한다.
- 결과 보고서 생성 기능이 있어야 하며, 점검 결과 분석을 통한 전체 네트워크 도메인의 보안성 평가를 해주고 가능한 공격을 예방하도록 보안관리에 대한 의사결정을 제시할 수 있어야 한다.
- 보안 정책 서버(Security Policy Server)와 연동하여 대규모 네트워크 도메인에 해당 조직의 보안 정책이 제대로 반영되었는지의 여부를 분석할 수 있어야 한다.
- 보안평가 시스템을 중앙에서 원격으로 쉽게 관리할 수 있어야 하고 중앙에서 전체 네트워크의 보안 상황을 한눈에 파악할 수 있어야 한다.
- 보안 관리 서버와의 연동을 통한 취약점 복구 기능, 전체 네트워크 보안수준 향상을 위한 보안관리 의사결정 지원 등을 제공하여야 한다.
- 신뢰할 수 있는 기관으로부터 새로운 취약점 정보를 수시로 얻어와 쉽게 이를 보안성 분석에 적용시킬 수 있어야 한다.

4.2 보안평가 시스템의 구조

위의 요구사항을 반영하여 본 논문에서 제안하는 보안평가 시스템의 구조는 그림 1과 같다. 보안평가 시스

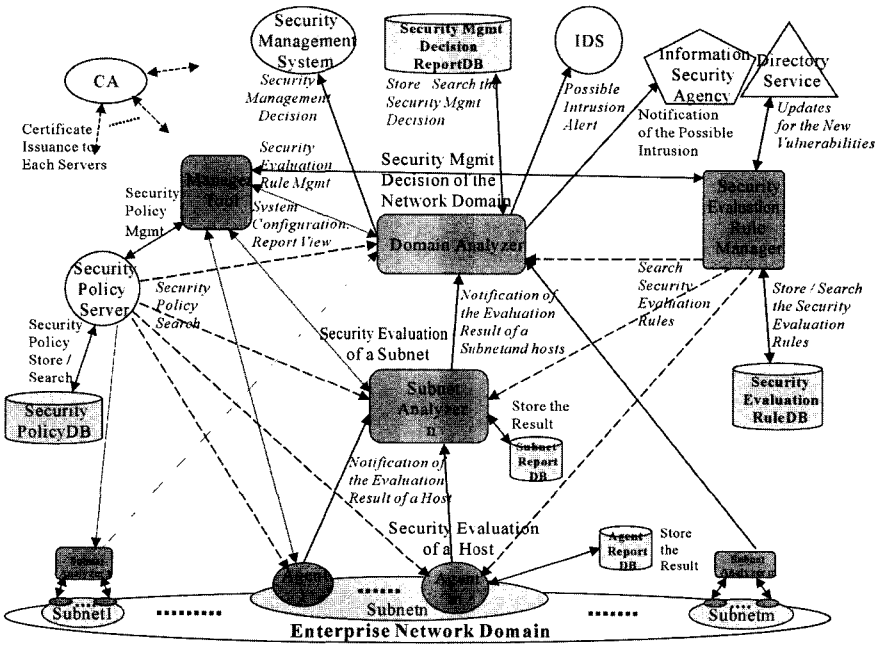

그림 1 보안평가 시스템의 구조

템을 구성하는 주요 요소는 에이전트(Agent), 서브넷 분석기(Subnet Analyzer), 도메인 분석기(Domain Analyzer), 보안평가 규칙 관리자(Rule Manager), 관리자 도구(Manager Tool) 등이다. 에이전트는 특정 호스트에 설치되어 해당 호스트의 보안성을 분석하여 그 결과를 서브넷 분석기에 통보하며, 서브넷 분석기는 네트워크 관점에서 자신이 속해 있는 서브넷의 보안성을 분석하고 그 결과를 도메인 분석기에 통보한다. 도메인 분석기는 각 에이전트 및 서브넷 분석기의 보안성 평가 결과를 토대로 네트워크 도메인 전체의 보안성을 평가하며 발견된 취약점에 대한 정보를 보안관리 시스템이나 침입탐지 시스템에 전달한다. 에이전트, 서브넷 분석기, 도메인 분석기 및 보안관리 시스템이나 침입탐지 시스템과 같은 외부 시스템 간의 보안성 분석 정보 흐름을 그림에서 실선으로 나타내었다.

에이전트, 서브넷 분석기, 도메인 분석기와 같은 보안성 분석 모듈은 보안성 분석 시 보안평가 규칙 관리자에 의해 관리되는 보안평가 규칙을 사용하며, 또한 보안정책 서버가 관리하는 보안정책을 참조하여 이를 보안성 평가에 반영한다. 보안성 분석 모듈과 보안평가 규칙 관리자, 보안정책 서버 간의 관계를 굵은 실선으로 나타내었다. 각 보안성 분석 모듈은 관리자 도구에 의해 관리되며, 이들 간의 관계를 가는 실선으로 나타내었다. 관리자 도구는 또한 보안관리자가 보안평가 규칙 관리자의 보안평가 규칙과 보안정책 서버의 보안 정책을 관리할 수 있도록 해주며, 이들 간의 관계를 실선으로 나타내었다. 그림의 각 모듈들에 대한 설명은 다음과 같다.

4.2.1 에이전트(Agent)

에이전트는 특정한 호스트 내부에서 수행되어 해당 호스트의 보안성을 하위 레벨의 상세한 사항까지 분석한다. 잘못된 시스템 설정, 해커의 침입 흔적, 시스템 파일의 무결성, 바이러스나 트로이 목마 존재 여부 등을 분석하여 호스트 보안성 평가 결과 보고서를 생성하고 이를 서브넷 분석기에 보낸다.

4.2.2 서브넷 분석기(Subnet Analyzer)

서브넷 분석기는 특정 서브넷의 네트워크 관점에서의 보안성을 평가한다. 취약한 네트워크 서비스 및 데몬 등을 분석하며, 해당 서브넷에 속해 있는 각 에이전트로부터 받은 호스트 보안성 평가 결과 보고서를 분석하여, 분산 환경을 구성하는 다수의 호스트에 관한 정보가 있어야 분석할 수 있는 보안상 취약점을 찾아낸다. 서브넷의 보안성 평가 결과는 도메인 분석기에 보내진다.

4.2.3 도메인 분석기(Domain Analyzer)

도메인 분석기는 각 에이전트 및 서브넷 분석기의 보안성 평가 결과를 토대로 대규모 네트워크 도메인 전체의 보안성을 평가한다. 각 호스트 및 서브 네트워크의 취약점 및 이들의 상관관계를 분석하여 이들 취약점으로 인해 발생할 수 있는 침입 가능성을 찾아내고 이를 막기 위한 보안관리 의사결정을 보안 관리자에게 제시해 주고 보안상 문제가 발견된 호스트의 관리자에게도 이에 대한 조치를 취하도록 메일을 발송한다. 발견된 취약점 및 이에 대한 보안관리 의사결정을 보안관리 시스템이나 침입탐지 시스템에 통보하여 적절한 방어 조치를 취하도록 해준다.

4.2.4 보안평가 규칙 관리자(Rule Manager)

보안평가 규칙 관리자는 보안 관리자가 보안평가에 필요한 규칙을 생성하고 관리하는 것을 도와준다. 보안평가 규칙은 특정 시스템 혹은 네트워크 자원과 관련된 취약점, 이로 인해 발생할 수 있는 보안상 위협 및 이에 대한 대응책으로 구성되며 에이전트, 서브넷 분석기, 도메인 분석기의 보안성 평가는 보안평가 규칙 관리자에 의해 관리되는 보안평가 규칙을 바탕으로 이루어진다. 신뢰할 수 있는 외부기관의 디렉토리 서비스로부터 수시로 새로운 취약점 정보를 가져와 이를 보안평가 규칙에 반영하여 보안평가시 새로운 취약점 정보가 즉시 활용될 수 있도록 한다.

4.2.5 관리자 도구(Manager Tool)

관리자 도구는 보안평가 시스템의 관리를 도와주며 보안 관리자는 이를 통해 각 구성 요소의 기능을 중앙 집중식으로 원격으로 설정하고 보안평가 규칙, 보안 정책 등을 관리한다. 관리자 도구는 보안 관리자가 보안관리 의사결정 결과 보고서를 다양한 형태로 조회할 수 있도록 해준다.

4.2.6 기타

보안평가 시스템의 각 구성 요소들은 보안평가 결과 등의 중요한 데이타를 주고받을 때 암호화를 적용하며, 서로간의 인증을 위해 인증기관(CA, Certificate Authority)으로부터 인증서를 발급 받아 사용한다.

보안정책 서버는 대규모 네트워크 도메인 전체에 대한 보안 정책을 저장하고 관리하는 서버이며, 보안평가 시스템은 보안평가시 항상 보안정책 서버를 통해 해당 네트워크 도메인의 보안정책을 참조하여 이의 충족여부를 분석함으로써 대규모 네트워크 도메인의 구성 요소들의 보안 설정이 항상 일관성을 갖도록 도와준다.

4.3 보안평가 시스템 설계의 특징

본 논문에서 제시하는 보안평가 시스템은 현재 시점에서의 대규모 네트워크의 보안성을 평가하여 이에 대한 정보 및 보안상 취약점을 제거하기 위한 보안관리 의사결정을 제시해주며, 보안평가 시스템의 각 분석 모듈 (에이전트, 서브넷 분석기, 도메인 분석기)에서의 보안성 분석은 보안평가 규칙 관리자에 의해 관리되는 보안평가 규칙을 바탕으로 이루어진다. 새로운 취약점이

알려질 경우에도 모듈 자체를 수정할 필요 없이 보안평가 규칙만 추가하면 되기 때문에 기능 확장이 용이하다. 또한 보안평가 규칙 관리자는 신뢰할 수 있는 기관의 디렉토리 서비스로부터 새로운 취약점 정보를 수시로 얻어와 보안평가 규칙에 반영되게 함으로써 보안평가에 새로운 취약점 정보가 신속히 적용되어 새로운 취약점에 대해 빠른 대처를 할 수 있다.

기존의 COPS와 같은 호스트 기반 취약점 분석 도구는 특정 호스트에 대해서는 높은 정확성과 신뢰도를 가지고 보안성을 분석해내지만 다수의 시스템을 효율적으로 관리하기 어렵고 한 곳에서 네트워크 전체의 보안성을 분석하기 어렵다는 단점이 있다. 반면 SATAN과 같은 네트워크 기반 취약점 분석 도구는 중앙에서 전체 네트워크의 보안성을 분석할 수 있지만 네트워크를 통해 접근할 수 없는 특정 호스트 내부의 취약성은 분석할 수 없다는 단점이 있다.

본 논문에서 제안한 시스템에서는 에이전트는 호스트 기반 취약점 분석을 수행하고, 서브넷 분석기와 도메인 분석기는 네트워크 기반 취약점 분석을 수행하고 각 에이전트의 보안성 분석 결과를 수집함으로써 각 호스트 내부의 취약성까지 정확히 분석할 수 있으면서 중앙에서 전체 네트워크의 보안성을 파악할 수 있다. 즉, 호스트 기반 보안성 분석과 네트워크 기반 보안성 분석의 장점을 모두 가지고 있다.

각 호스트에 설치된 에이전트를 이용하여 호스트 기반 보안성 분석을 수행할 경우 새로운 취약점 정보가 생길 경우 각 호스트에 설치된 에이전트를 수정해야 한다는 문제가 발생할 수 있다. 하지만 본 논문의 설계에서는 보안평가 규칙 관리자에 의해 관리되는 보안평가 규칙을 기반으로 보안성 평가를 하기 때문에 각 호스트에 설치된 에이전트를 수정할 필요 없이 보안평가 관리자가 새로운 보안평가 규칙을 추가하기만 하면 새로운 취약점 분석을 수행할 수 있다. 이러한 특징은 특히 규모가 큰 네트워크에서는 커다란 장점이 될 수 있다.

기존의 네트워크 기반 취약점 분석 도구나 에이전트/매니저 구조로 되어 있는 취약점 분석 시스템은 네트워크 상의 호스트 수가 많아질 경우 매니저에 많은 부하가 걸리게 되는 문제가 발생한다. 하지만 본 논문에서 제시된 보안평가 시스템은 보안성 평가를 하나의 분석 모듈에서 수행하지 않고 에이전트, 서브넷 분석기, 도메인 분석기를 단계적으로 거쳐 수행함으로써 특정 모듈에 걸리는 부하를 최소화하고 네트워크 도메인의 호스트 수가 증가하더라도 에이전트와 서브넷 분석기의 개수를 늘리면 시스템의 성능이 별로 저하되지 않는 확장성을 갖는다. 또한 시스템을 조사한 결과가 모두 도메인 분석기에 전달되지 않고 에이전트 및 서브넷 분석기에서 보안상 문제가 되는 것만 걸러내어 보내주므로 상대적으로 네트워크 트래픽이 적어지고 매니저에 해당하는 도메인 분석기의 데이타 처리량이 줄어들게 되어 대규모 네트워크 환경에 적합하다.

또한 보안평가 시스템은 보안성 분석 시 해당 네트워크 도메인의 보안 정책을 참조하여 네트워크 구성요소들의 보안정책 충족 여부를 함께 분석함으로써 대규모 네트워크 도메인 전체의 보안 정책 준수 여부를 쉽게 판별할 수 있다.

4.4 보안평가 시스템의 세부 구조 및 수행 절차

보안평가 시스템의 대략적인 수행절차는 다음과 같다. 보안평가 규칙 데이타베이스(rule DB)의 업데이트는 보안관리 의사결정과는 별도로 수시로 일어난다.

① 에이전트에 의한 각 호스트 보안성 분석
② 서브넷 분석기에 의한 각 서브넷 보안성 분석
③ 도메인 분석기에 의한 네트워크 도메인의 보안 관리 의사결정

보안평가 시스템의 각 분석 모듈(에이전트, 서브넷 분석기, 도메인 분석기)에서 보안성 평가는 다음과 같은 절차로 처리된다.

① 보안평가 규칙 및 보안정책을 근거로한 시스템 혹은 네트워크 자원 조사 및 분석
② 보안평가 결과 보고서 생성
③ 상위 분석 모듈에 결과 전달

보안성 분석시 보안평가 규칙뿐만 아니라 보안정책의 충족 여부도 분석하여야 한다. 이를 위해 먼저 보안평가 규칙 데이타베이스 및 보안정책 데이타베이스에서 분석 대상인 특정 호스트 혹은 네트워크와 관련된 항목만을 골라내어 이를 맞춤 규칙 데이타베이스(Customized Rule DB)에 저장하고 이 맞춤 규칙(Customized Rule)을 사용하여 보안성 평가를 수행한다. 만약 이전에 동일한 시스템 환경 및 동일한 보안평가 규칙, 동일한 보안정책으로부터 생성된 맞춤 규칙이 있으면 규칙 데이타베이스 및 보안정책 데이타베이스로부터 새로 규칙을 액세스하지 않고 이미 생성되어 있는 맞춤 규칙을 사용하여 데이타베이스 액세스 시간 및 검색 시간을 줄인다. 보안평가 규칙과 보안 정책 사이에 서로 충돌되는 사항이 있으면 보안정책을 우선적으로 따른다.

보안평가 시스템의 세부 구조 및 구체적인 수행 절차는 다음과 같다.

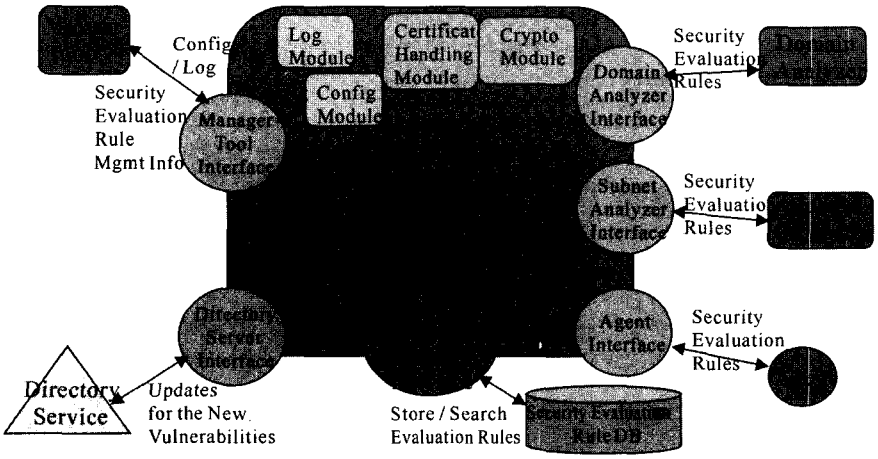

그림 2 보안평가 규칙 관리자의 구조

4.4.1 보안평가 규칙 관리자에 의한 보안평가 규칙 데이타베이스 생성

보안평가 규칙 관리자의 구조는 그림 2와 같다. 보안평가 규칙 관리자는 외부의 신뢰할 수 있는 기관의 디렉토리 서비스로부터 새로운 취약점 정보를 수시로 가져오며, 보안평가 규칙 생성기(Security Evaluation Rule Generator)는 관리자 도구를 통해 보안 관리자가 내린 보안평가 규칙 처리 명령에 따라 이 취약점 정보로부터 보안평가 규칙을 생성하고 이를 보안평가 규칙 데이타베이스에 저장한다. 보안 관리자는 관리자 도구를 사용하여 보안평가 규칙을 추가, 삭제, 변경할 수 있다.

에이전트, 서브넷 분석기, 도메인 분석기는 보안평가 규칙 관리자의 보안평가 규칙을 사용하여 보안성 평가를 수행하며, 규칙 관리자는 이들이 보안평가 규칙을 요청하면 해당 보안평가 규칙을 보안평가 규칙 데이타베이스로부터 검색해 각각에 대한 인터페이스 모듈을 통해 전달한다.

4.4.2 에이전트에 의한 각 호스트 보안성 분석

에이전트의 구조는 그림 3과 같다. 각 에이전트의 맞춤 규칙 생성기(Rule Customizer)는 보안정책 서버와 보안평가 규칙 관리자로부터 해당 호스트의 환경에 맞는 보안평가 규칙과 보안 정책을 액세스하여 이를 맞춤 규칙 데이타베이스(Customized Rule DB)에 저장한다. 만약 데이타베이스에 이전에 생성된 호스트 맞춤 규칙(Customized Host Rule)이 존재하고 운영체제, 네트워크 프로토콜 등의 시스템 환경이 동일하며 보안평가 규

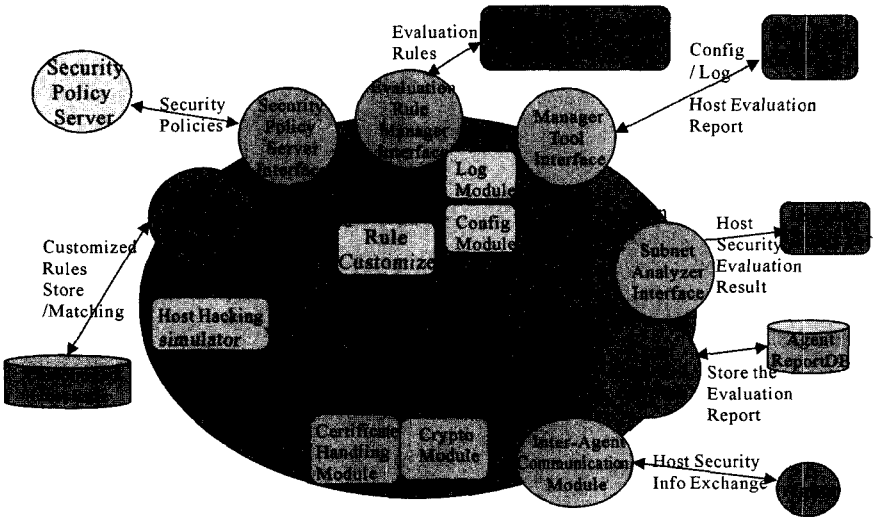

그림 3 에이전트의 구조

칙, 보안정책이 변하지 않았다면 이 과정을 생략하고 기존의 호스트 맞춤 규칙을 사용한다.

호스트 검사 엔진(Host Check Engine)은 호스트 맞춤 규칙을 바탕으로 해당 호스트의 보안성을 평가하며, 다른 호스트에 관한 정보가 있어야 분석할 수 있는 보안상 허점을 찾아내기 위해 에이전트들 간에 서로 특정 호스트에 대한 정보를 교환할 수도 있다.

또한 호스트 해킹 시뮬레이터(Host Hacking Simulator)를 사용하여 로컬 호스트에 대한 취약성을 검사해보며, 이때는 반드시 시스템에 로그를 남겨 실제 해킹 시도와 구별되도록 한다. 이 과정에서 시스템 설정 상태, 버그 패치 여부, 해커 침입 흔적, 바이러스나 트로이 목마, 스니퍼의 존재 여부, 해당 호스트의 보안정책 충족 여부 등이 조사된다. 에이전트 보고서 관리자(Agent Report Manager)는 호스트 검사 엔진의 보안성 평가 결과를 근거로, 발견된 보안상 취약점과 이에 대한 대책 등의 정보를 포함하는 호스트 보안성 평가 결과 보고서를 생성하여 에이전트 보고서 데이타베이스(Agent Report DB)에 저장하고 서브넷 분석기에게도 이 보고서를 전달한다.

4.4.3 서브넷 분석기에 의한 각 서브넷 보안성 분석

서브넷 분석기의 구조는 그림 4와 같다. 기존의 서브넷 맞춤 규칙(Customized Subnet Rule)이 존재하지 않으면 각 서브넷 분석기의 맞춤 규칙 생성기(Rule Customizer)는 해당 서브넷의 환경에 맞는 보안평가 규칙과 보안정책을 액세스하여 이를 서브넷 맞춤 규칙 데이타베이스(Customized Subnet Rule DB)에 저장한다.

서브넷 검사 엔진(Subnet Check Engine)은 서브넷 맞춤 규칙을 바탕으로 해당 서브넷의 보안성을 평가하며, 이때 다른 서브넷에 관한 정보가 필요할 때 해당 서브넷 분석기와 정보를 교환하기도 한다. 또한 네트워크 해킹 시뮬레이터를 사용하여 네트워크를 구성하는 리모트 호스트에 대한 취약성을 검사해보며, 이때는 반드시 해당 시스템에 로그가 남도록 하여 실제 해킹 시도와 구별되도록 한다. 네트워크 서비스 및 데몬 등의 보안성을 분석하고 에이전트 보고서 분석기(Agent Report Analyzer)를 이용해 해당 서브넷에 속해 있는 에이전트들의 호스트 보안성 분석 결과 보고서를 분석하여 서브넷을 구성하는 각 호스트의 보안성 평가를 종합하고 분산 환경을 구성하는 다수의 호스트에 걸쳐 존재하는 보안상 취약점을 분석해낸다. 이때 해당 네트워크 도메인의 보안정책 충족 여부도 함께 분석된다. 서브넷 보고서 관리자(Subnet Report Manager)는 서브넷 검사 엔진의 보안성 평가 결과를 근거로, 발견된 보안상 취약점과 이에 대한 대책 등의 정보를 포함하는 서브넷 보안성 평가 결과 보고서를 생성하여 서브넷 보고서 데이타베이스(Subnet Report DB)에 저장하고 도메인 분석기에게도 이 보고서를 전달한다.

4.4.4 도메인 분석기에 의한 대규모 네트워크 보안관리 의사 결정

도메인 분석기의 구조는 그림 5와 같다. 도메인 분석기의 맞춤 규칙 생성기(Rule Customizer)는 전체 네트워크 도메인 보안성 분석에 맞는 보안평가 규칙과 보안정책을 액세스하여 이를 도메인 맞춤 규칙 데이타베이스(Customized Domain Rule DB)에 저장한다.

보안관리 의사결정 엔진(Security Management Decision Engine)은 도메인 맞춤 규칙(Customized Domain Rule) 및 각 서브넷 및 호스트의 보안성 평가 결과를 바탕으로 전체 네트워크의 보안성을 평가하여 취약점으로 인해 발생 가능한 침입을 분석하고 이를 예

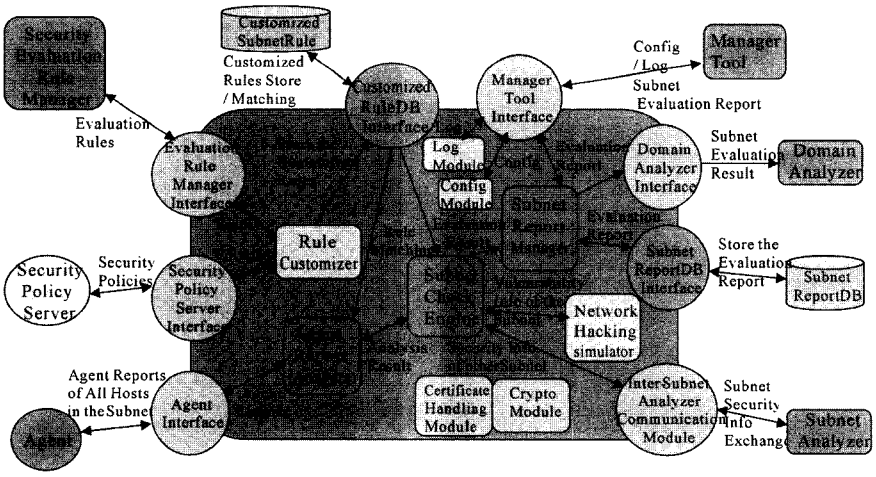

그림 4 서브넷 분석기의 구조

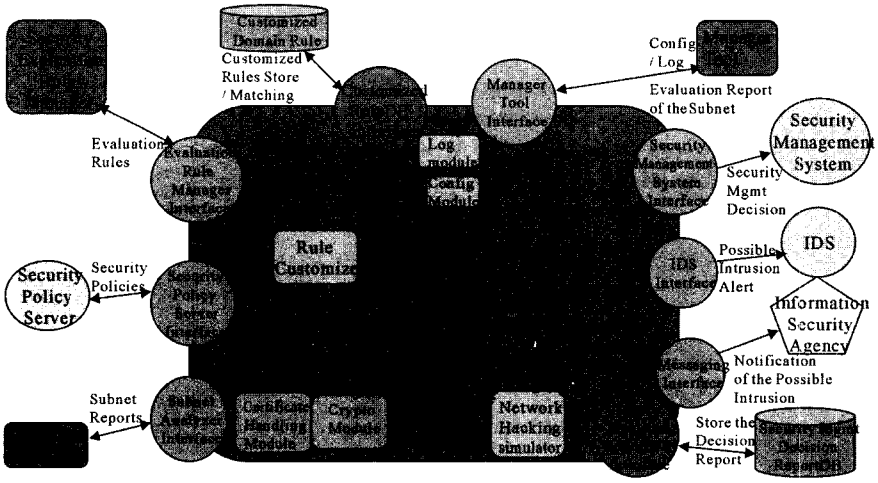

그림 5 도메인 분석기의 구조

방하기 위한 보안관리 의사결정을 내린다. 이를 위해 서브넷 보고서 분석기 (Subnet Report Analyzer)를 이용하여 해당 도메인에 속해 있는 서브넷 분석기의 서브넷 보안성 분석 결과 보고서를 통합 분석하여 전체 네트워크의 보안성을 분석해 내고 다수의 서브넷 및 호스트에 걸쳐 존재할 수 있는 보안상 취약점을 추가로 분석하며 각 에이전트 및 서브넷 분석기의 분석결과중 중복된 항목을 합치고 잘못 분석된 항목을 제거한다.

보안관리 의사결정 보고서 관리자(Security Management Decision Report Manager)는 보안관리 의사결정 엔진의 보안관리 의사결정 결과로부터 보고서를 생성하여 보안관리 의사결정 보고서 데이타베이스(Security Management Decision Report DB)에 저장한다. 보안관리자는 관리자 도구를 사용하여 이 보고서를 조회하여 보안관리 의사결정에 활용할 수 있다.

도메인 분석기는 발견된 취약점 및 이에 대한 보안관리 의사결정을 보안관리 시스템이나 침입탐지 시스템에 알려주어 가능한 공격에 대한 조치를 취하게 한다. 보안관리 시스템에는 적절한 시스템 설정 변경을 요청하며 침입탐지 시스템에는 침입 가능성을 알려준다. 심각한 침입 흔적이 발견되었을 경우 관련 기관에 이에 관한 통지 메일을 발송하며 취약점이 발견된 시스템의 관리자에게도 적절한 조치를 취하도록 메일을 보낸다.

4.4.5 관리자 도구를 이용한 결과 조회

보안 관리자는 관리자 도구를 통해 보안평가 시스템의 각 구성 요소의 기능을 중앙 집중식으로 원격으로 설정하고 보안평가 규칙, 보안 정책 등을 관리하며 보안관리 의사결정 지원 보고서를 다양한 형태로 조회할 수 있다. 관리자 도구의 세부구조는 그림 6과 같다.

관리자 도구는 사용자 인터페이스(User Interface)를

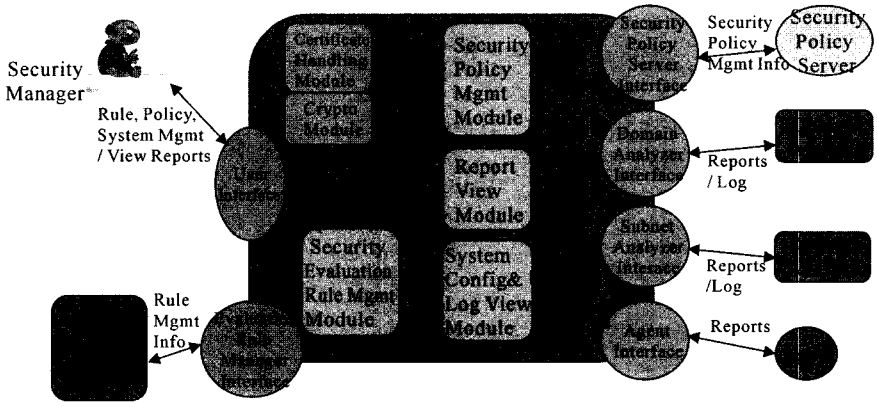

그림 6 관리자 도구의 구조

통해 보안 관리자의 요청을 받아 적절한 처리 모듈을 호출하고 결과를 출력한다. 보안 정책 관리 모듈(Security Policy Management Module)을 통해 보안 정책 서버의 보안 정책을 수정하거나 추가하고, 보고서 조회 모듈(Report View Module)을 통하여 결과 보고서를 다양한 형태로 변환하여 출력한다. 또한 보안평가 규칙 관리 모듈(Security Evaluation Rule Management Module)을 통해 보안관리 규칙 관리자(Security Evaluation Rule Manager)의 규칙을 추가하거나 삭제한다. 시스템 설정 및 로그 조회 모듈(System Configuration & Log View Module)을 사용해 각 구성요소의 시스템 설정을 하거나 로그를 출력할 수도 있다.

5. 결 론

본 논문에서는 다양한 요소로 구성된 대규모 네트워크 환경에서의 네트워크의 보안성 평가를 자동화하고 침해사고 예방을 위해 보안관리 의사결정을 도와주는 보안평가 시스템에 대한 요구 사항을 분석하고 이를 반영한 보안평가 시스템을 설계하였다.

본 논문에서 제안한 보안평가 시스템은 호스트 기반 보안성 분석 도구와 네트워크 기반 보안성 분석 도구의 장점을 모두 가지고 있어 네트워크를 이용해서는 분석할 수 없는 특정 호스트의 취약성을 정확히 분석할 수 있고 대규모의 네트워크에서도 네트워크 전체의 보안성 분석을 쉽게 수행할 수 있다.

보안규칙을 기반으로 보안성을 분석하며 새로운 취약점 정보가 알려질 경우 네트워크 상의 모든 에이전트들을 수정할 필요 없이 보안규칙 관리자에서 새로운 보안 규칙을 추가하기만 하면 새로운 취약점 분석을 수행할 수 있으며, 이러한 특징은 대규모의 네트워크 환경에서는 커다란 장점이다.

제안된 보안평가 시스템은 디렉토리 서비스로부터 새로운 취약점 정보를 수시로 얻어와 보안평가 규칙에 반영할 수 있도록 하여 새로운 취약점에 대해 신속하게 대처할 수 있도록 설계되었다. 이 시스템은 대규모 네트워크를 구성하는 각 호스트 및 서브넷의 보안성 분석 결과를 종합하여 전체 네트워크 도메인의 보안 수준을 평가하고 보안상 취약점을 해결하기 위한 보안관리 의사결정을 지원해 준다. 이때 보안평가가 에이전트, 서브넷 분석기, 도메인 분석기를 단계적으로 거쳐 수행되게 함으로써 매니저 역할을 하는 모듈에 걸리는 부하를 적게 하였고 네트워크 도메인 내부의 호스트 수가 증가하더라도 에이전트와 서브넷 분석기의 개수를 늘리면 시스템의 성능이 저하되지 않는 확장성을 갖도록 설계하였다. 또한 시스템을 조사한 결과가 모두 도메인 분석기에게 전달되지 않고 에이전트 및 서브넷 분석기에서 보안상 문제가 되는 것만 걸러내어 보내주므로 네트워크 트래픽이 비교적 적고 도메인 분석기의 데이타 처리량이 대폭 줄어들어 대규모의 네트워크 환경에 적합하도록 설계하였다. 보안평가 규칙 데이타베이스 및 보안정책 데이타베이스로부터 특정 시스템에 맞도록 최적화된 맞춤 규칙을 생성하여 사용함으로써 보안성 분석시의 처리효율을 높이도록 하였으며 보안평가 시스템은 보안정책을 참조하여 보안평가를 하므로 네트워크 도메인 전체가 보안 정책을 어느 정도 준수하고 있는지 쉽게 파악할 수 있다.

보안평가 시 보안정책을 참조해야 하지만 아직 보안정책 기술에 대한 연구가 부족하고 표준도 없는 상태이기 때문에 이에 대한 많은 연구가 필요하며 보안평가 규칙을 이용한 보안성 평가에 보다 정확하고 유연한 판단을 내리고 특정 취약점이 발견되었을 경우 이로 인해 발생되는 침입을 예측하기 위하여 전문가 시스템 등의 인공지능 기법 적용에 대한 연구도 필요하다.

참 고 문 헌

[1] Simson Garfinkel & Gene Spafford, Practical UNIX & Internet Security, O'REILLY, Second Edition, April 1996.

[2] Sundaram Aurobindo, "An Introduction to Intrusion Detection," ACM CROSSROADS Issue 2.4, 1996.4.

[3] Daniel Farmer, Eugene H. Spafford, "The COPS Security Checker System," Purdue University Technical Report CSD-TR-993, Jan 1994.

[4] Larry J. Hughes, Jr., Actually Useful Internet Security Techniques, New Riders Publishing, 1995.

[5] Nessus Project Home Page, http://www.nessus.org/

[6] Symantec Enterprise Solutions Home Page, http://enterprisesecurity.symantec.com

[7] ISS Vulnerability Assessment Products Home Page, http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/index.php

[8] Shostack, A., S. Blake., "Toward a Taxonomy of Network Security Assessment Techniques," Proceedings of the 1999 Black Hat Briefings, July 1999.

[9] S. J. Shin, J. W. Yoon and B. M. Lee, "A Prototype Design of Expert System for Automated Risk Analysis tool," Proceedings of the 10th Workshop on Information Security and Cryptography, pp. 383-395, 1998.

[10] ISS, "Network and Host-based Vulnerability Assessment," http://documents.iss.net/whitepapers/nva.pdf

[11] ISS, "Securing Operating Platforms: A solution for tightening system security," January 1997.

[12] Farmer, D. and W. Venema, "Security Administrator Tool for Analyzing Networks," http://

www.fish.com/satan
[13] Baldwin, R. W., "Rule-Based Analysis of Computer Security," Massachusetts Institute of Technology, Cambridge, MA, June 1987.
[14] 이재승, 김상춘, 이종태, 김경범, 손승원, "대규모 네트워크 환경하에서의 침해사고 예방을 위한 보안평가 시스템 설계", 제12회 정보보호와 암호에 관한 학술대회(WISC2000), 160~176, 2000. 9.
[15] 한국전산원, 정보시스템 보안을 위한 위험분석 소프트웨어 개발 보고서, 1997.
[16] S. W. Kim, H. J. Jang and B. Park, "Dynamic Monitoring based on Security Agent," Proceedings of the 10th Workshop on Information Security and Cryptography, pp.518-530, 1998.

이 재 승

1993년 서강대학교 수학과 졸업(이학사) 1997년 포항공과대학교 정보통신학과 졸업(공학석사). 1997년 3월~1999년 데이콤 정보통신연구소(연구원). 1999년 8월~현재 한국전자통신연구원 정보보호연구본부(연구원). 관심분야는 전자상거래 정보보호, 네트워크 정보보호, 암호학

김 상 춘

1986년 한밭대학교 전자계산학과(공학사) 1989년 청주대학교 전자계산학과(공학석사). 1999년 충북대학교 전자계산학과(이학박사). 1983년~2001년 한국전자통신연구원 정보보호기술연구본부(선임기술원) 2001년 4월~현재 삼척대학교 정보통신공학과 조교수