실시간 e-mail 대응 침입시도탐지 관리시스템의 설계 및 구현

박 수 진† · 박 명 찬† · 이 새 롬†† · 최 용 락†††

요 약

인터넷의 발전과 더불어 해킹기법 또한 함께 발전하고 있다. 최근의 검색공격 형태는 한 기관의 네트워크를 대상으로 하기보다는 상위 도메인을 대상으로 대규모적인 공격 형태를 지니고 있다. 실질적으로 대응하기 위해서는 중앙시스템에서 취약점 검색공격을 탐지, 분석하고 조치할 수 있는 시스템이 있어야 한다. 침입시도탐지 관리시스템은 현재 국내 주요기관들에 설치된 다수의 침입시도탐지 시스템들로부터 받은 여러 탐지 정보를 실시간으로 수집 분석하여 효과적으로 이용하는데 유용하다. 대규모 네트워크의 환경에 적절한 구조를 갖으며 보다 고수준의 통합된 분석을 할 수 있는 실시간 침입시도탐지 관리시스템을 개발하였다.

Design and Implementation of A Scan Detection Management System with real time Incidence Response

Soo-Jin Park† · Myung-Chan Park† · Sae-Rom Lee†† · Yong-Rak Choi†††

ABSTRACT

Nowadays, the hacking techniques are developed increasingly with wide use of internet. The recent type of scanning attack is appeared in against with multiple target systems on the large scaled domain rather than single network of an organization. The development of scan detection management system which can detect and analyze scan activities is necessary to prevent effectively those attacking at the central system. The scan detection management system is useful for effective utilization of various detection information that received from scan detection agents. Real time scan detection management system that can do the integrated analysis of high level more that having suitable construction in environment of large scale network is developed.

키워드 : RTSD(Real Time Scan Detector), 침입시도탐지 관리시스템(Scan Detection Management System), 침입탐지메시지교환형식(IDMEF), 침입경고 메일(Incidence Response Mail)

1. 서 론

최근 네트워크 보안 취약점을 자동으로 검색해주는 mscan, sscan과 같은 보안 관리도구들이 개발되어 공개되고 있다. 해커들은 이런 자동화된 보안 관리도구들을 공격도구로 이용하여 침입하고자 하는 시스템의 보안 취약점 정보 및 공격대상을 찾는데 활용하고 있다. 침입 후에 탐지를 하는 방법보다는 침입을 하기 위해 사전에 해보는 일들을 미리 탐지하는 침입시도탐지가 적극적인 예방차원에서 더욱 필요하게 되었다[4, 7, 12]. 이러한 네트워크 취약점 검색공격에 대응하기 위하여 scanlogd, gabriel, snort등 다양한 형태의 프로그램이 인터넷에 공개되고 있으나, 이러한 시스템은 대부분 다양한 대규모 네트워크 검색공격을 모두 탐지하지 못할 뿐만 아니라 공격에 대한 적절한 대응 수단을 제공하지 않는다. 또한 최근의 검색공격 형태는 한 기관의 네트워크를 대상으로 하기보다는 상위 도메인을 대상으로 대규모적인 공격 형태를 지니고 있다. 이에 효과적으로 대응하기 위해서는 여러 침입시도탐지시스템에서 취약점 검색공격을 탐지한 자료를 받아 대응할 수 있는 중앙에 관리시스템이 있어야 한다[17]. 따라서 본 논문에서는 이를 위해 대규모 네트워크의 환경에 적절한 구조를 갖으며 e-mail로 대응하는 침입시도탐지 관리시스템을 설계 및 개발하였다.

침입시도탐지 관리시스템은 제안한 메시지 형식에 맞게 보내는 각 침입시도탐지 에이전트들의 탐지 정보를 효과적으로 활용하며, 에이전트들을 운영, 관리한다. 또 웹 기반으

† 준 회 원 : 대전대학교 대학원 컴퓨터공학과
†† 정 회 원 : 한국정보보호진흥원 기반보호사업단 해킹바이러스상담지원센터
††† 종신회원 : 대전대학교 컴퓨터공학과 교수
논문접수 : 2002년 3월 18일, 심사완료 : 2002년 5월 7일

로 실시간 탐지 관련 정보를 검색할 수 있으며, 분석결과에 의해 침입시도로 판단되는 주소는 Whois를 통해 그 네트워크 관리 담당자에게 이메일을 보내 대응할 수 있다.

본 논문은 2장에서 서로 다른 종류의 시스템들 간의 메시지 상호호환을 위해 IETF(The Internet Engineering Task Force)에서 제안하고 있는 침입탐지 메시지 교환형식에 대해 기술하고, 3장에서는 에이전트들과 탐지 메시지 교환을 위한 침입시도탐지 메시지형식과 침입시도탐지 관리시스템의 구성 및 설계에 대해 기술한다. 4장에서는 침입시도를 탐지한 후 통계서비스 및 공격 네트워크 관리자에게 이메일을 보내는 대응에 대해 실행한 결과들을 보여준다. 마지막으로 5장은 결론 및 향후 연구를 기술한다.

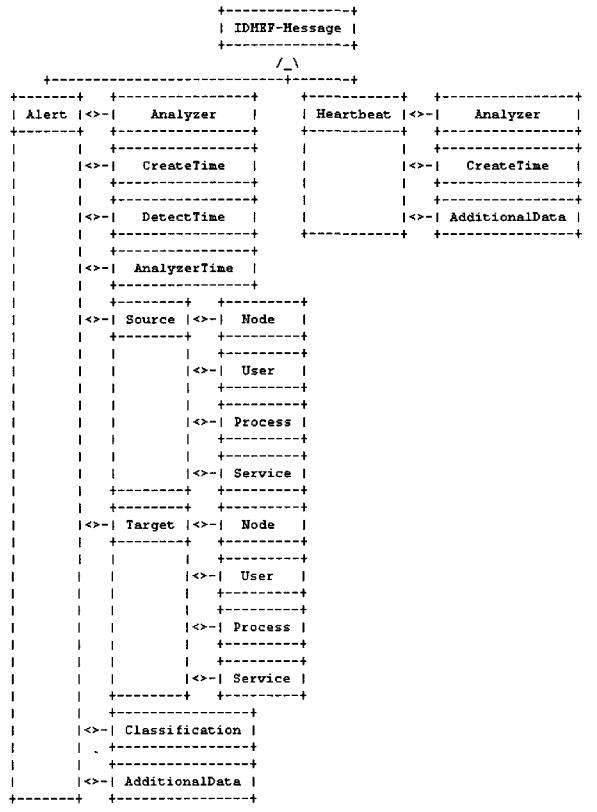
2. 관련 연구

침입탐지 메시지 교환 형식 IDMEF(Intrusion Detection Message Exchange Format)는 서로 다른 종류의 시스템들 간의 메시지 상호호환을 위하여 IETF에서 제안하고 있는 침입탐지 시스템들간의 표준 메시지 교환 형식이다. 침입시도탐지 시스템에서 IDMEF로 표현할 수 없는 메시지들을 교환하기 위해 먼저 IDMEF를 분석했다.

2.1 침입탐지 메시지 교환 형식

IDMEF는 IETF에서 제안하고 있는 메시지 교환 형식으로서, 침입탐지 시스템과 그 응답 시스템 및 관리시스템간에 정보를 공유하기 위한 데이터 형식과 교환 절차를 정의한다. 서로 다른 종류의 탐지 시스템간의 메시지의 상호 호환을 위하여, IDMEF는 표준의 메시지 교환 형식을 정의하는데, 그 데이터 모델을 UML(Unified Modeling Language)로 정의하고 XML(Extensible Markup Language)을 사용하여 구현하고 있다[5].

(그림 1)에서 최상위 클래스는 IDMEF-Message로서 Alert와 Heartbeat의 두 가지 하위 클래스로 분류된다. Alert와 Heartbeat는 다시 여러 클래스를 포함하고 각 클래스들은 속성을 갖는다. Alert 클래스는 침입을 탐지했을 경우 그 경보를 정의하는 부분이다. Analyzer는 탐지한 분석자의 정보를 표현하며, CreateTime은 Alert를 생성한 시간, DetectTime은 침입을 탐지한 시간, AnalyzerTime은 서버쪽 시간과 동기화를 하기 위해 현재의 Analyzer 시간을 나타낸다. 또 침입을 한 Source와 침입을 당한 Target 클래스가 있다. Source 클래스 내에는 호스트나 디바이스에 대한 정보를 나타내는 Node, 유저에 대한 정보를 나타내는 User, 이벤트를 발생시킨 과정에 대한 Process와 그리고 어떤 네트워크 서비스를 사용했는지에 대한 Service를 하위 클래스로 가지고 있다. Target 클래스도 Source 클래스가 가지고 있는 하위 클래스들을 똑같이 가지고 있다. Classification은 어떤 침입인지를 분류하기 위한 클래스이다. AdditionalData 클래스는 위의 다른 클래스들에 쓰지 못한 추가하고 싶은 내용들을 넣는 클래스로 어떤 데이터 타입이든지 가능하다.



(그림 1) IDMEF의 데이터 모델

Heartbeat 클래스는 하위 클래스로 분석자의 정보인 Analyzer, Heartbeat를 생성한 시간인 CreatTime, 추가정보를 넣기 위한 AdditionalData를 갖는다.

IDMEF는 UML로 정의된 데이터 모델의 각 클래스와 속성들의 표현 형식과 관계를 XML의 DTD(Document Type Definition)로 정의한다.

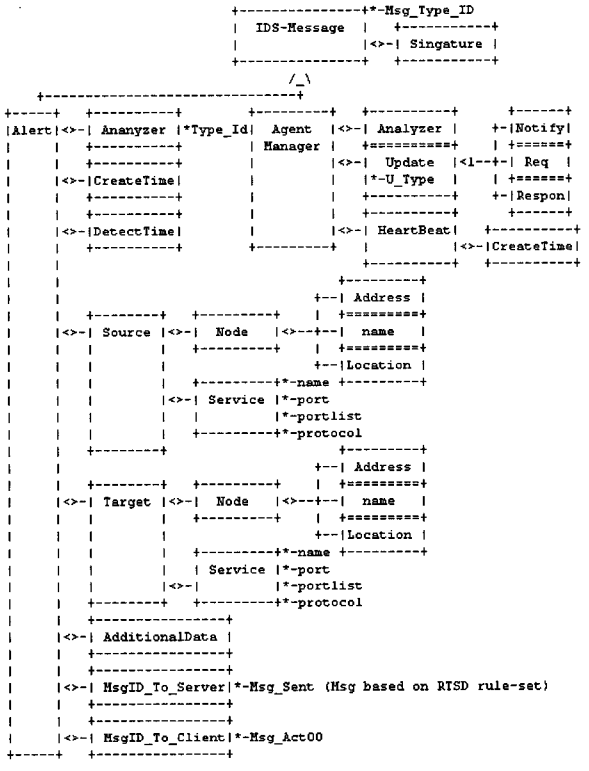
3. 침입시도탐지 관리시스템 설계

3.1 침입시도탐지 메시지 교환 형식

IDMEF는 침입탐지 메시지 교환을 위한 형식이기 때문에 침입시도탐지 메시지 교환에서 필요로 하는 침입시도 대응 메시지, 업데이트 공지, 업데이트 요청, 침입보고, Active 상태 보고와 같은 부분은 충족시키지 못한다. 이런 부분을 충족하기 위하여 (그림 2)와 같은 데이터 모델을 구성하였으며, CERTCC-KR(Korea Computer Emergency Response Team Coordination Center)에서 개발한 RTSD(Real Time

Scan Detector)와 연결하여 관리한다.

최상위 클래스는 IDMEF-Message로서 Alert와 Heartbeat의 두 가지 하위 클래스로 분류된다. IDMEF-Message는 Signature 클래스와 Msg_Type_ID를 갖는다. Msg_Type_ID는 메시지 타입을 간단히 표현하여 나중에 데이터베이스에서 정보를 분류하기 용이하도록 하기 위해 추가되는 속성이며 메시지를 다루는데 있어서 첫 번째 요소가 된다. 또한 Signature 클래스를 두어 인증 부분을 넣을 수 있도록 하였다. Alert 클래스는 IDMEF 모델과 유사하나 Source와 Target에서 User와 Process 부분을 제외한 Node와 Service 클래스 부분만을 구현하였다. 또 Classification 클래스 대신 서버에게 보내는 메시지인 MsgID_To_Server와 클라이언트에서 보내는 메시지인 MsgID_To_Client로 나누었다. 또 Heartbeat는 Agent Manager 클래스의 하위 클래스로 두어 Agent 관리에 관한 내용들을 더 많이 추가할 수 있도록 하였다. Agent Manager 클래스는 분석자, 또 업데이트 요청에 관한 부분과 HeartBeat 부분으로 구성되어 있다.



(그림 2) 침입시도탐지 메시지 교환 형식

<표 1>은 침입탐지 메시지 교환 형식에서 확장된 클래스와 삭제된 클래스를 분류하였다.

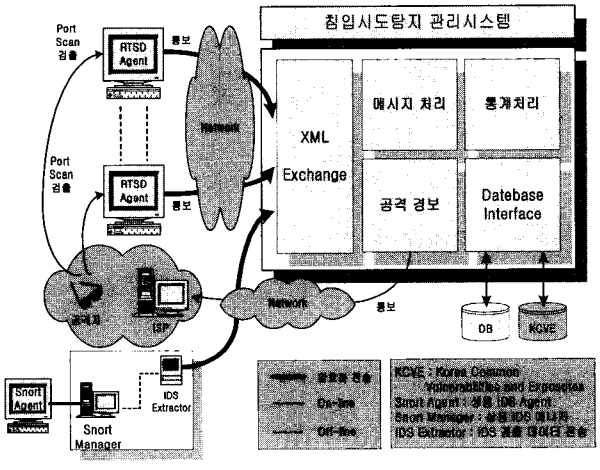
<표 1>과 같이 침입탐지 메시지 교환 형식을 확장 및 삭제하여 침입시도탐지 시스템에 맞게 새롭게 구성하였다. 확장된 부분은 Alert 클래스에서 MsgID_to_Server 클래스를 두어 침입시도탐지 시스템으로부터 1차적인 탐지 결과를 획득할 수 있으며, 에이전트의 Additionaldata를 heartbeat로 변경 RTSD의 활동 상태를 확인할 수 있다.

〈표 1〉 메시지 교환 형식 분석

구분	Class	하위 Class	내 용
확장	Alert	MsgID_to_Server	RTSD로부터 공격유형 통보
		MsgID_to_Client	공격에 대한 대응 정보 통보
	Agent Manager	Update	RTSD Update 정보
		HeartBeat	RTSD 등록 정보
삭제	Alert	AnalyzerTime	DetectTime에 포함
		Classfication	MsgID_to_Server에 포함
	Agent	Create Time	Update 변경
		AdditionalData	HeartBeat 변경

3.2 관리시스템 구성

침입시도탐지 관리시스템은 각 네트워크 단위로 감시하는 침입시도탐지 시스템으로부터 탐지된 메시지를 받아서 재분석하여 전 네트워크를 감시한다. CERTCC-KR에서 국내 정보시스템 해킹공격시도 현황을 파악하고 이에 적극 대응하기 위하여 RTSD 개발하였다. RTSD는 "한 호스트로부터 일정 시간(TIME_DELAY_THRESHOLD)동안 일정한 수(SCAN_COUNT_THRESHOLD) 이상의 연결 요청이 있을 경우 이를 침입시도로 탐지" 알고리즘으로 탐지를 한다. 호스트 기반의 취약점 검색 탐지기법에서는 포트를 대상으로 탐지를 하지만, RTSD는 소스 IP만을 대상으로 하여 각 네트워크에 하나씩 설치되어 그 네트워크를 침입시도하는 것을 탐지 할 수 있다. 최근의 검색공격 형태는 한 기관의 네트워크를 대상으로 하기보다는 상위 도메인을 대상으로 다수의 경로 사이트들에 대한 동시적 공격 형태를 지니고 있다. 그러므로 각 네트워크 내에서 탐지한 메시지들을 중앙 관리시스템으로 보내어 대규모 네트워크 침입시도를 탐지한다. 앞 절에서 확장 제안하여 개발한 메시지 교



(그림 3) 시스템 구성도

환 형식을 사용한다면 다른 침입시도탐지 시스템과의 연결도 가능하다[3, 6, 10]. 전체적인 침입시도탐지 관리시스템의 구성도는 (그림 3)과 같다.

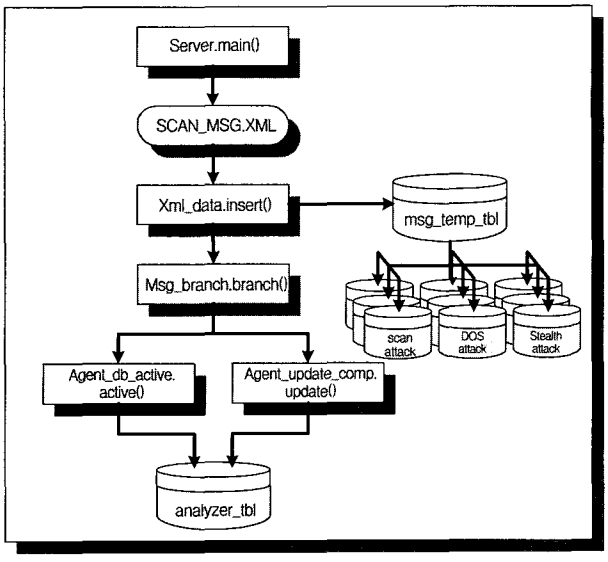
침입시도탐지 관리시스템은 분산된 침입시도탐지 시스템으로부터 실시간으로 XML형태의 탐지 정보를 수신하여 DB에 저장을 한다[1, 8]. DB는 3개로 구성되어 있는데 침입시도탐지 시스템들로부터 수신된 모든 탐지 정보들은 정보 DB에 저장되고, 이 메시지를 분석하여 메시지가 침입시도탐지 시스템의 상태보고라든지 업데이트에 관련된 메시지인 경우 에이전트 관리 DB로, 침입시도탐지 관련 메시지인 경우 통계 DB로 저장된다. 통계 DB를 바탕으로 일별, 월별, 년별 또는 공격포트별, 프로토콜별 통계정보를 제공한다. 또 공격지의 네트워크 관리자에게 경고 메일을 발송한다.

3.3 상세 모듈 설계

침입시도탐지 관리시스템은 탐지 메시지 처리 모듈과 탐지 메시지 통계처리 모듈 그리고 공격 경보 모듈로 분류된다.

3.3.1 탐지 메시지 처리

탐지 메시지 처리 모듈은 침입시도탐지 시스템으로부터 탐지 정보를 수신하고 메시지 타입에 따라 침입시도탐지 시스템의 관리 및 탐지 정보에 대한 공격 유형별, 프로토콜별로 분류하여 해당 데이터베이스 테이블에 저장한다. (그림 4)는 탐지 메시지 처리 클래스 구성도를 보여준다.



(그림 4) 탐지 메시지 처리 클래스 구성도

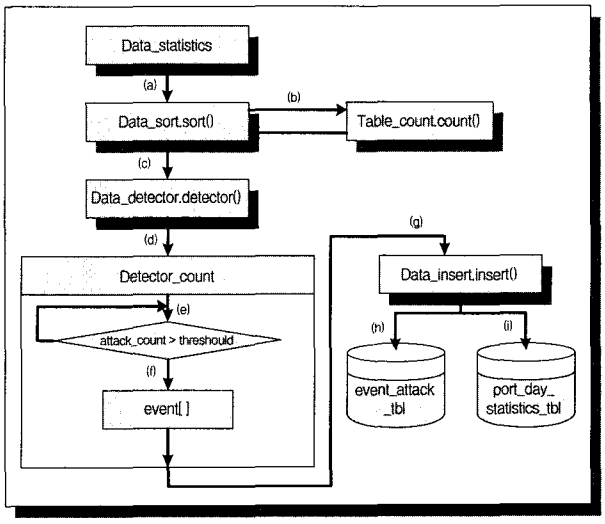
Server.main()에서는 RTSD Agent로부터 수신된 탐지 정보를 수신하여 SCAN_MSG.XML을 생성한다. Xml_data.insert( )에서는 SCAN_MSG.XML 파일을 XML 파서 프로그램을 이용하여 오라클 DB에 입력한다. 데이터 입력시 오라클 내부에 이미 정의 된 Trigger에 의해서 각 공격유형, 프로토콜별로 분류되어 저장된다. <Msg_branch.branch( )>는 미리 정해놓은 Msg_Type에 의해 해당 클래스를 호출한다.

Msg_type == 0인 경우는 Active 보고 기능을 수행하고, Active 보고 기능은 RTSD Agent의 현재 상태 정보를 관리시스템에 송신함으로써 RTSD의 상태를 통보한다.

Msg_Type == 1인 경우는 Update 요청을 수행하고, Update 정보를 확인하기 위하여 <agent_update_comp.update( )>는 수신된 RTSD의 버전 정보와 공지된 버전을 비교한다.

3.3.2 탐지 메시지 통계처리

탐지 메시지 처리 모듈에서 처리된 각 공격 유형별 빈도수를 바탕으로 실제 공격에 대하여 판별한다. 이때, 공격에 대한 판별 기준은 각 공격 타입에 따라 차이가 있다. SCAN 공격은 일정시간 동안 하나의 공격 주소와 하나의 공격 포트가 같고, 목적지 주소가 다른 탐지 정보가 임계값 이상 발견되면 이를 SCAN 공격으로 간주한다. (그림 5)은 메시지 통계처리 클래스 구성도를 보여준다.



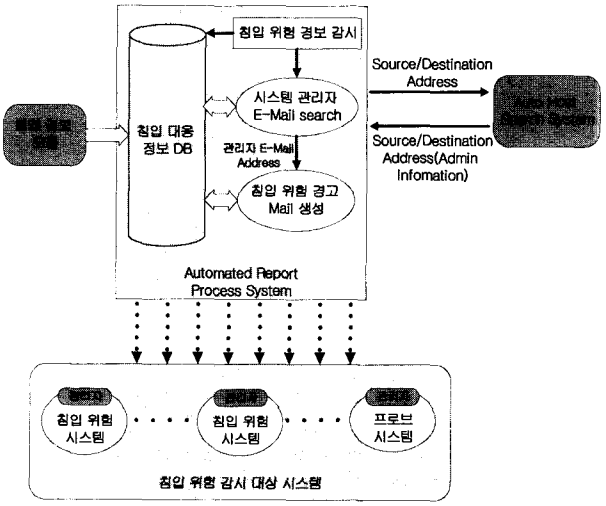
(그림 5) 메시지 통계처리 클래스 구성도

<Data_statistics()>는 탐지 메시지 처리 모듈에서 분류된 정보 중 일정패턴을 검색한다. 먼저 일정패턴을 검색하기 위하여 저장된 탐지 정보를 검색하여 일정한 순서로 정렬한다. <Data_sort.sort()>는 탐지 정보를 각 공격 유형별 DB에서 검색하여 탐지 시간 및 공격지 주소, 목적지 포트 순으로 정렬한다. <Data_detector.detector()>는 <Table_count.count()>에서 얻어진 데이터 수만큼 반복하며 일정시간 동안 같은 공격지 주소와 같은 목적지 포트를 가진 다수의 탐지 정보를 수집한다. Detector_count에서 수집된 정보 중 Threshold 이상의 탐지 정보가 발견되면 이를 공격으로 간주한다. 공격으로 판별된 검색 정보는 event[ ]에 해당 탐지 정보와 함께 저장된다. 모든 값에 대하여 반복 수행한다.

저장된 event[ ]에 저장된 탐색 정보를 [event_attack_tbl]에 저장하고 통계정보를 위하여 [port_day_statistics_tbl] 저장한다.

3.3.3 침입시도 대응 모듈

탐지 메시지 통계처리 모듈에 의해서 판별된 공격에 대하여 공격지에 경고 메일을 발송한다. 공격자에게 직접 경고 메일을 보내기 위해서는 공격자의 메일정보를 알고 있어야 하기 때문에 불가능하다. 침입시도 대응 모듈은 탐지 메시지 통계처리 모듈에서 판별된 공격정보를 바탕으로 공격자의 IP를 가지고 Whois 서비스를 이용하여 그 공격자가 속해있는 네트워크 관리자의 메일정보를 알아내어 공격 경보메일을 발송한다. 침입 대응/경고 모듈은 (그림 6)과 같다.



(그림 6) 침입 대응/경고 모듈

각각의 침입경보 모듈, 침입대응 정보DB, 침입위험경보 감시, 침입위험경고 메일 생성, 시스템 관리자 E-Mail Search, Auto Host Search System에 대한 설명은 <표 2>와 같다.

〈표 2〉 침입 대응 자동처리 모듈

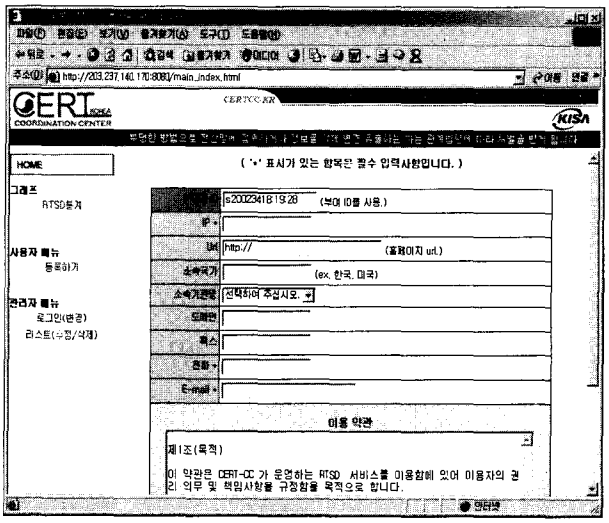
모듈 이름	기 능
침입경보 모듈	• 침입위험이 감지된 시스템 정보를 침입 대응 정보DB에 저장
침입대응 정보DB	• 침입위험 시스템 로고 및 IP Address • 위험경고 메시지 • 침입위험 시스템 관리자 등록 정보
침입위험 경보 감시	• 침입위험 시스템 이벤트 감시
침입위험 경고 E-Mail 생성	• 침입위험 시스템 경고 메시지 생성
시스템 관리자 E-Mail Search	• 침입위험 시스템 관리자 등록 정보를 Auto Host search System에 요청 후 E-Mail Address 발췌
Auto Host Search System	• IP Address 등록 관리자 등록 정보 서비스 시스템

침입위험 시스템 정보 및 IP Address가 임시 폴더 보관함에 저장되면 임시 폴더 감시 모듈 이벤트가 발생하여 Whois 모듈이 작동된다. Whois 모듈은 임시 폴더에 위험 시스템 정보 파일을 읽고 보낼 편지함에 저장하며, 침입위험 시스템 IP Address를 발췌한다. 이 IP Address를 자동 "Whois" 검색 서버에 관리자 등록 정보를 요청하고 관리자 E-Mail Address 발췌하여 경고 메시지를 생성한다. 침입위험 메시지를 자동으로 보내기 전에 오경보를 줄이기 위하여 메일 관리자가 직접 판단 후 삭제 및 전송을 한다. 전송한 경고메일은 보낸 편지함에 저장된다[2, 9, 11].

4. 침입시도탐지 관리시스템 실행

4.1 사용자 등록 서비스

침입시도탐지 관리시스템의 웹서비스는 크게 두가지로 분류된다. (그림 7)과 같이 RTSD를 다운 받아 사용하는 사용자들의 정보를 등록하는 서비스와 침입탐지통계를 검색할 수 있는 서비스이다. 웹을 통한 사용자등록은 RTSD의 관리 및 서비스지원을 한다.

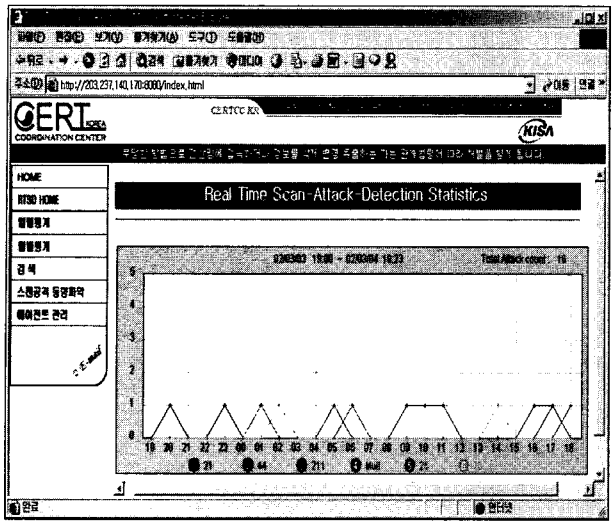


(그림 7) 사용자 등록 서비스

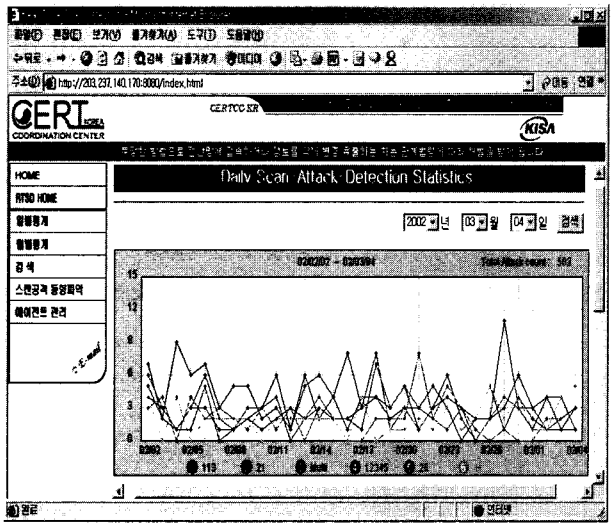
4.2 통계정보 제공 서비스

침입시도탐지 정보를 웹으로 실시간이나 원하는 날짜로 검색할 수 있는 서비스이다. 일별, 월별, 프로토콜별 통계정보를 제공하며, attack_event_tbl, port_day_statistics_tbl, port_month_statistics_tbl에 저장된 정보를 Query 함으로써 얻어진다.

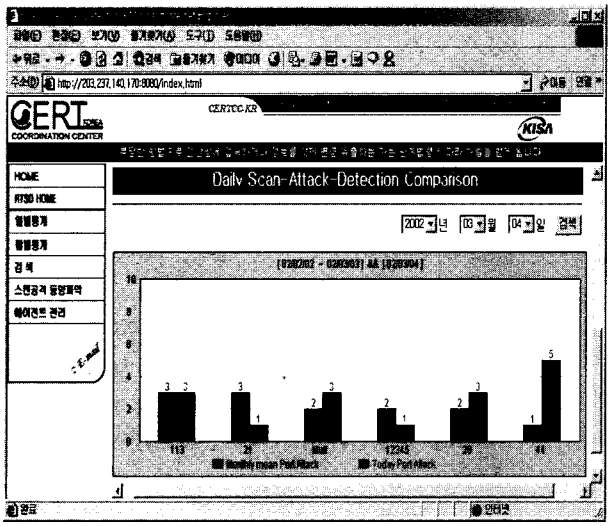
(그림 8)과 같이 현재 본 순간부터 하루 전까지 가장 많이 침입시도 되었던 포트를 6개까지 보여주며, 매 시간별로 침입시도 되었던 포트들의 횟수를 보여준다. ❶Multi는 하나의 공격지에서 다수의 포트로 침입시도를 한 정보를 나타낸다.



(그림 8) 실시간 침입시도탐지 통계 그래프



(그림 9) 일별 침입시도탐지 통계 그래프



(그림 10) 일별 침입시도탐지와 평균 비교

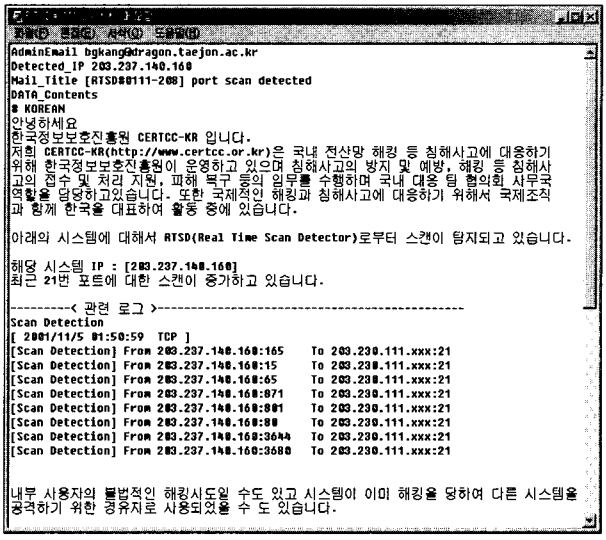
(그림 9)의 통계 정보는 검색하고 싶은 날짜를 선택하면 선택한 날부터 한달 전까지 일별로 침입시도 되었던 포트들의 정보를 보여주며, 한달 동안 많이 침입시도 되었던 포트들의 정보를 보여준다.

(그림 10)의 통계정보는 검색하고 싶은 날짜를 선택하면 그 날짜로부터 한달 전까지의 침입시도 평균과 그 날의 침입시도를 비교한다. 한달 평균 침입시도가 높은 순서로 표시된다. 포트 검색 기능이 있어 검색하고 싶은 날의 포트를 최대 6개까지 검색할 수 있으며, Whois기능으로 알고싶은 Address를 입력하면 그 Address에 대한 정보를 알 수 있다.

4.3 공격 대응 메일 서비스

임시 폴더에 이벤트 파일이 생성되면 이를 검출, 파싱하여 "Whois" 서비스를 이용, 공격지에 대한 관리자 메일 정보를 획득한다. 그후 보낼 편지함으로 자동 이동한다.

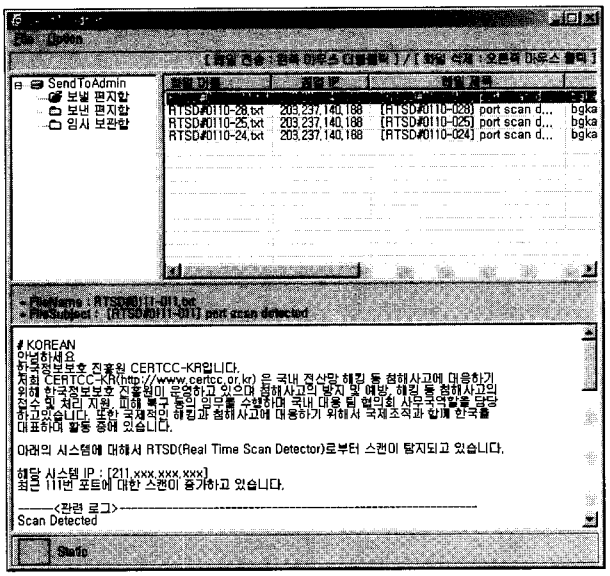
임시 폴더는 새로운 침입 위험 시스템 정보 파일이 저장된다. 이 파일은 (그림 11)과 같으며 시스템 위험이 감지된 날짜와 시간 순서로 번호가 주어진다.



(그림 11) 공격 경보 메일

위험경고 감시 프로세스는 임시 폴더를 감시하고 새로운 정보에 대해서 이벤트를 발생한다. 이벤트에 의해 관리자 E-Mail Address를 위험 정보에 추가하고, 이 정보는 보낼 편지함에 저장된다. 또한 이 저장된 파일은 관리자에 의해 관리되어 삭제 및 메일 전송이 이루어진다.

관리자는 (그림 12)와 같이 보낼 편지함을 클릭 함으로써 메일을 발송할 수 있으며 발송된 메일은 보낸 편지함으로 자동 이동한다. 공격정보를 포함하고, 관련 대응 정보를 제공하고 있다. 또한 탐색된 탐색정보를 함께 보내주어 탐지 정보의 신뢰성을 높여주고 있다.



(그림 12) 경보 메일 전송을 위한 보낼 편지함

5. 결 론

본 논문에서는 CERTCC-KR에서 국내 정보시스템 해킹 공격시도 현황을 파악하고 이에 적극 대응하기 위해, 대규모 네트워크의 환경에 적절한 구조를 갖으며 실시간 분석을 할 수 있는 침입시도탐지 시스템들을 관리하는 침입시도탐지 관리시스템을 설계 및 개발하였다.

침입시도탐지 시스템들로부터 정형화된 메시지를 받아 분석하고, 분석한 결과를 웹 페이지로 실시간 확인할 수 있는 서비스와 침입시도를 하는 네트워크 관리자에게 이메일로 대응한다. 메시지는 침입탐지 시스템들간의 표준화된 메시지 교환의 필요성으로 IETF에 제안된 IDMEF를 침입시도탐지시스템에 맞게 확장하여 제안하였다. 또한 효율적인 이메일 대응을 위해서 탐지된 주소를 가지고 Whois를 통하여 탐지된 주소를 포함한 네트워크 관리자에게 메시지와 탐지된 주소를 이메일로 전송한다.

침입시도탐지 관리시스템은 여러 소스 IP에 대한 분산 공격과 같은 다양한 침입시도 방법에 대한 탐지와 자동 경고 및 대응 메일 발송, 실시간 통계 현황을 통해 사이버테러의 조기 예방과 대응을 위한 시스템으로 기대된다. 또한 IDMEF를 따른 침입시도탐지 시스템과 침입시도탐지 관리시스템의 통신 방식 표준화로 후에 snort와 같은 IDS와의 연동이 가능한 확장된 시스템으로 발전될 것이다.

향후에는 각각의 침입시도탐지 시스템에서 전송되는 수많은 결과보고를 효율적으로 축약 및 관리하는 방법, 탐지 메시지에 대한 자동화 된 분석에 대한 좀더 많은 연구를 통해 침입에 대한 좀더 지능적인 예방 및 대응을 통한 대규모 네트워크 공격 탐지가 가능한 시스템으로의 확장이 필요하다.

참 고 문 헌

[1] W. Timothy Polk, "Automated Tools for Testing Computer System Vulnerability," 1992.

[2] Marc Farley, Tom Searns, Jeffrey Hsu, "Data Integrity and Security," Mc Graw-Hill, 1997.

[3] The Art of Port Scanning, Phrack Magazine Vol.7, Issue 51 September, 1997.

[4] Mscan 분석 보고서, CERTCC-KR, 김상정, 1998.

[5] INTERNET ENGINEERING TASK FORCE, Intrusion Detection Exchange Format Charter. Published electronically at, http : //www.ietf.org/html.charters/idwg-charter.html, 1998.

[6] Designing and Attacking Port Scan Detection Tools, Phrack Magazine Vol.8, Issue 53, article 13 of 15, July, 1998.

[7] Sscan 분석 보고서, CERTCC-KR, 정현철, 1999.

[8] NETWORK ASSOCIATES INCORPORATED, Proprietary Vulnerability Database for CyberCop Scanner 2.4., 1999.

[9] Network Scanning Techniques, Sys-Security Group, Ofir Arkin, 1999.

[10] "CERTCC-KR 보안 권고문", CERTCC-KR, 한국정보보호센터, http : //www.certcc.or.kr/advisory/adv_certcckr.html.

[11] Protecting against the unknown, Mixter, January, 2000.

[12] know Your Enemy : I, II, III, Lance Spitzner, 2000.

[13] 네트워크 공격기법의 패러다임 변화와 대응방안 Version 1.0, SecurityMap Network, 이현우, 2001.

박 수 진

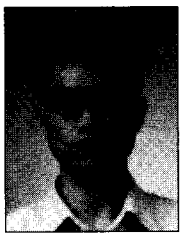
e-mail : sjpark@zeus.dju.ac.kr

1997년 한밭대학교 제어계측공학과 졸업 (공학사)

1999년 아주대학교 대학원 컴퓨터공학과 졸업(공학석사)

1999년~현재 대전대학교 대학원 컴퓨터 공학과 박사과정

관심분야 : 침입탐지, 보안API, 네트워크 보안



박 명 찬

e-mail : mcpark@zeus.dju.ac.kr

1999년 대전대학교 컴퓨터공학과 졸업 (공학사)

2001년 대전대학교 대학원 컴퓨터공학과 졸업(공학석사)

2001년~현재 대전대학교 대학원 컴퓨터 공학과 박사과정

관심분야 : 침입탐지, IPSec, 암호 컴포넌트

이 새 롬

e-mail : saerom@cert.certcc.or.kr

1998년 서울여대 수학과 졸업(이학사)

2001년 서울여대 대학원 컴퓨터학과 졸업 (이학석사)

2001년~현재 한국정보보호진흥원 기반 보호사업단 해킹바이러스상담 지원센터 재직

관심분야 : 침입탐지, 방화벽, 네트워크 보안

최 용 락

e-mail : yrchoi@dju.ac.kr

1976년 중앙대학교 전자계산학과 졸업 (공학사)

1982년 중앙대학교 대학원 전자계산학과 졸업(공학석사)

1989년 중앙대학교 대학원 전자계산학과 졸업(공학박사)

1986년~현재 대전대학교 컴퓨터공학과 정교수

2001년~현재 대전대학교 공과대학 학장

2001년~현재 한국정보보호학회 재무이사

관심분야 : 시스템 보안, 네트워크 보안, 보안API, PKI