분산 환경에서 정보보호 연관 경고 메시지를 이용한 ESM 구현

(An Implementation of ESM with the Security Correlation Alert for Distributed Network Environment)

한 근 희 † 전 상 훈 †† 김 일 곤 ††† 최 진 영 ††††
(Keun-Hee Han) (Sang-Hun Jeon) (Il-Gon Kim) (Jin-Young Choi)

요 약 본 논문에서는 각 센서에서 수집한 수 많은 경고 메시지중에서 불필요한 정보는 필터링하여, 위험 상태를 크게 4가지의 유형으로 분류하는 SIA 시스템을 제안하고 구현하였다. 또한 제안한 방법을 실제 환경에서 구현하여 현장에서 적용해 본 결과, 실시간으로 이루어지는 네트워크의 위험요소 판정에 도움을 줌으로써 보안관리자가 실질적인 위협에 즉각적으로 대처 할 수 있음을 확인하였다.

키워드 : ESM(Enterprise security Management), SIM(Security Information Management), CAM (Correlation Alert Message), SIA(Security Information Alert)

Abstract In this paper, we propose and implement SIA System for filtering redundant alert messages and dividing them into four statuses. Also, we confirm that our system can find and analyze vulnerability types of network intrusion by attackers in a managed network, so that it provides very effective means for security managers to cope with security threats in real time.

Key words : ESM(Enterprise security Management), SIM(Security Information Management), CAM(Correlation Alert Message), SIA(Security Information Alert)

1. 서 론

일반적으로 컴퓨터 시스템과 통신망의 침입 위협 예방과 방지를 위해 IDS와 Firewall 등의 보안 시스템이 구축되며, 네트워크를 통해 전달되는 대량의 정보 데이타에서 피해를 일으킬 수 있는 위험요소를 차단하고 탐지하게 된다[2]. 공격 기법의 변화와 복잡성이 증가함에 따라 하나의 침입기술이나 한차례의 공격보다 여러 개의 공격이 동시다발적으로 발생하고 있는 것이 일반적인 현상이다. 예를 들어 2001년의 Nimda 바이러스의 경우 이메일 공격과 네트워크 공유 공격, CodeRed 바이러스의 백도어 공격, Unicode 공격 등 여러 가지 형태의 혼합된 공격 패턴을 포함하고 있으며 동시에 진행되는 형태였으나[1], 현재까지의 정보 보호 시스템에서 이 모든 공격을 특정(Nimda, Slammer, SQL Worm, Code Red) 바이러스라고 연결지어서 알려주는 정보보호 시스템은 없다. 일개 단위의 침입에 대해서는 경보를 발생시키고 알려 주지만 종합적인 정보를 제공하지 못함으로로써 다양한 방법을 혼합한 침입에 대하여 효과적으로 대응을 하기에는 어려움이 존재하였다. 정보보호와 관련하여 수집되는 방대한 데이타들로 인해 데이타의 분석을 통해 실제적인 위협요소를 판별하고 침입을 차단, 방지하는 과정에 많은 시간이 소요되게 되며 판단과 분석과정에서 사람의 개입과 많은 전문인력이 필요하게 되었다. 이러한 과정을 개선하기 위해 여러 논문에서 다양한 방안으로 접근을 하고 있다. IDS 로그를 혼합(Hybrid) 형태로 판별하기 위한 시도로 [1],[2]는 침입 경보를 상호연관(correlation)시켜 거짓 경고(False alert)를 줄임으로써 실제적인 위협요소를 줄이려는 방안을 제시했고, [1],[3]에서는 분산된 환경에서의 침입 탐지 이벤트를 추상화하였고 공격에 대한 계층적 모델을 제공하였다. 그리고 [3],[4]에서는 데이타웨어 하우징(Dataware housing)과 데이타마이닝(Datamining) 기법

† 정 회 원 : 건국대학교 정보통신대학원 교수
khhan@formal.korea.ac.kr
†† 비 회 원 : SK infosec 전임 컨설턴트
winsnort@securityindepth.net
††† 학생회원 : 고려대학교 컴퓨터학과
igkim@formal.korea.ac.kr
†††† 종신회원 : 고려대학교 컴퓨터학과 교수
choi@formal.korea.ac.kr
논문접수 : 2003년 8월 28일
심사완료 : 2003년 12월 15일

을 이용하여 복잡화된 공격을 판별 할 수 있도록 제시하였다. 위의 논문에서는 다양한 경고(alert)의 통합과 실제적인 위협을 판별할 수 있도록 하였으나 IDS와 Firewall을 통합한 상호연관관계 경고의 생성 및 실제 위협의 판단을 위한 데이타의 제공 여부는 고려되어 있지 않다.

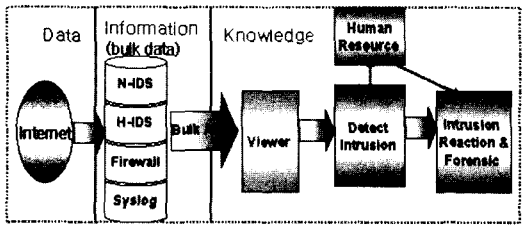


그림 1 현재 침입 탐지 패러다임

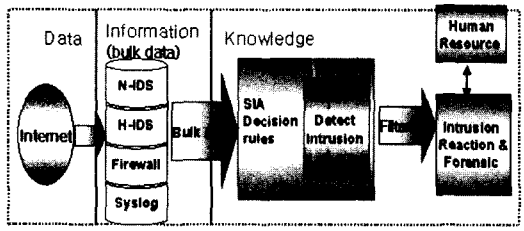


그림 2 SIA 로직을 이용한 새로운 침입탐지 패러다임

본 논문에서는 IDS와 Firewall 경고 메시지에 대한 상호연관관계 경고를 제공하고, 위협이 증가하고 있는 DDoS(Distributed Denial of service) 공격의 탐지[5]에 상호연관관계 경고가 어떤 형태로 기여하는지를 보이고 기반 데이타의 제공을 통해 실제 위협이 발생했을 경우 신속히 판단하여 대응할 수 있도록 새로운 알고리즘과 보호모델을 시험하고 구현하였다. 또한 침입탐지 시스템 자체의 거짓 경보(False alarm)와 각각의 보안 시스템 경고와 이벤트의 형식이 달라서, 일목요연한 침입의 판단과 다수의 보안시스템이 설치된 네트워크상에서 종합적인 침입에 대한 인지가 어려운 실정이다. 대부분의 ESM(Enterprise Security Management) 혹은 SIM(Security Information Management)[6]에서 기본 구현이 실질적인 침입의 인지보다 보안장비에 대한 종합적인 관리차원에서 단순히 수집한 정보만 관리자에게 보여주도록 구현되어 있어서 보안시스템이 동작하고 있는 네트워크에서 침입유형과 위험도를 즉각적으로 인지하지 못함으로서, 사실상 네트워크와 시스템에 대한 침입의 의도와 탐지를 신속하고 정확하게 탐지해 내지 못하고 있다.

본 논문에서는 각 센서에서 수집한 로그 정보를 표준 포맷으로 바꾼 후, 일반적인 침입의 모델을 새로운 방식으로 정의하고 분류하여 침입의 의도와 대상에 따라 정확한 목적을 인지함으로써 보안 관리자가 신속하게 공격자의 침입 유형에 대응할 수 있도록 SIA 시스템을 설계하고 구현하였다. 본 논문에서 제안한 알고리즘을 활용하여 멀티센서(IDS, Firewall 로그들)들로부터 수집한 대량의 경고 메시지를 사람이 직접 분석하여, 위험도를 판단하는 하는 대신(그림 1), 위협에 대한 사항을 축약하여 간단명료하게 알려줌으로써(그림 2), 인적 자원에 대한 의존도를 상당부분 줄이면서 신속하고 정확하게 판단하고 즉각적으로 대응할 수 있음을 보여주고 있다. 특히 기존에 구축된 보안시스템의 침입 탐지 데이타를 이용해 다수의 대상에 대한 공격 혹은 단일 대상에 대한 집중적인 공격 및 취약점을 스캐닝할 수 있으며, Firewall과 IDS 로그를 종합 분석함으로써 침입자에 대한 추적과 공격의도를 유추하기 쉽도록 설계하였다.

본 논문의 구성은 다음과 같이 이루어져 있다. 2장에서는 SIA(Security Information Alert) 시스템 모델의 배경 및 이와 유사한 연구 활동에 대해서 언급하고 현재 발표되어 있는 보안 시스템들의 상태에 대해서 설명할 것이다. 3장에서는 본 논문에서 새로이 제안한 공격탐지 판단의 기준이 되는 간단한 평가 로직에 대해 설명하고, 멀티센서 로그의 정보통합을 위한 표준 포맷에 대해 언급한다. 4장에서는 제안된 모델을 이용한 실제적인 구현과 실제 환경에서 실험한 결과에 대한 성능비교 분석 결과를 보여준다. 마지막으로 5장에서는 향후 연구 내용과 제안한 시스템의 성능향상을 위해 추가적으로 필요한 사항에 대해 설명하도록 하겠다.

2. ESM(SIM 또는 SEM) 관련 연구

기존의 멀티센서에서 얻어지는 경고 혹은 이벤트로부터 유용한 정보를 도출하려는 연구가 진행되어 왔다. 이런 연구는 기존의 보안 솔루션에 대한 통합 분석요구에서부터 시작되었으며, 전문가적인 상황 해석 능력이 필요함에 따라 더욱 고도화가 요구되고 있다. 멀티센서들로부터 수집한 경고 메시지와 이벤트의 포맷은 각 제조업체마다 저마다 다르게 사용하고 있어서 종합적인 분석에 있어서 포맷의 불일치와 동일한 공격에 대해 각각 다른 표현방식을 사용함으로써 정보보호 관리자에게 큰 혼란을 주고 있다[4]. 이러한 문제를 해결하기 위해 각 센서에서 발생하는 경고 메시지와 이벤트를 기반으로 통합된 결과를 얻으려는 연구가 진행되고 있다. 그 중에서 호스트 기반 IDS와 네트워크 기반 IDS에서 발생하는 경고 메시지와 이벤트를 통합하기 위한 솔루션의 형태를 메타 IDS(그림 3)라고 부른다[6,7]. 메타 IDS는 호스트와 네트워크 침입 탐지 센서로부터 수집한 경고 데이타를 하나의 관리자 콘솔에 나타내며, 모든 보안 장비

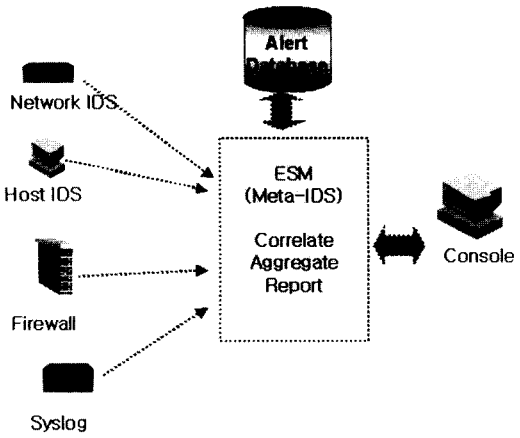


그림 3 Meta-IDS

로부터 발생되는 데이타와 유용한 정보, 보안 경고 메시지를 관리가 인식 가능한 형태의 표준 포맷으로 받아드리는 시스템을 의미한다. 메타 IDS를 구축하기 위해서는 경고 데이타베이스(Alert Database)가 필수적으로 요구된다. 또한 이를 구성하기 위해서는 멀티센서로부터 발생되는 경고 메시지에 대하여 표준 포맷을 정의하고 경고 데이타베이스를 만들어 상호연관관계를 도출하는 것이 중요하다.

메타 IDS를 구성하기 위한 두 가지 시도가 이루어지고 있다. 첫 번째는 각각의 상이한 경고 메시지에 대한 표준 포맷 작성이고, 두 번째는 각 센서에 플러그인 형태로 보안 경고를 제품에 맞는 포맷으로 변환하는 모듈을 내장하는 형태로 연구가 진행되고 있다. 제한적인 표준 포맷의 사용 및 플러그인 형태로 포맷을 변환하고 정보를 보내는 제품으로는 CheckPoint사에서 제안한 OPSEC(Open Platform Security), NAI(Network Associates, Inc)의 Active Security, IBM의 Tivoli Secureway Risk Manager 등이 있다.

현재까지 구현되어 있는 ESM(메타 IDS) 모델은 에이전트를 통한 메시지 통합과, 각 센서에서 독자적인 방식으로 메시지를 받아서 처리하는 형태를 가지고 있어서, 서로 다른 제품의 경우에는 표준 포맷으로 변환하여 활용하기에 시간 및 비용의 소모가 크다.

다양한 보안시스템의 경고 메시지를 통합하는 ESM 모델에서 필수적으로 요구하는 구성요소는 3가지가 있다.

1) 통제(Control): 보안 정책에 따른 멀티센서 통제 기능
2) 위협(Threat): 위협요소를 확인한 후, 대응하는 기능
3) 상호연관관계(Correlation): 보안 경고 메시지를 수집, 상호연관 과정을 거쳐 근본 원인을 찾아내는 기능

예를 들어 Motorola사의 MIV(Motorola Intrusion Vision)는 10여개의 IDS로부터 경고 메시지를 수집하여 한 화면에 요약 분석해 주고, 대응방법을 제시해 주지만 IDS의 경고 메시지로만 제한되어 있다. 이러한 문제점을 보완하고 메시지를 통합하는 방안으로 표준화 작업이 진행 중에 있다. 종합적인 침입 탐지 정보의 획득을 위한 표준 포맷에 대한 연구가 IDWG(Intrusion Detection Exchange Format Working Group)[8]에서 이루어지고 있다. 공통된 포맷을 이용하여 멀티센서에서 탐지한 정보의 형식을 일정형태로 일치시키고 변환의 편리를 위해 XML 타입으로 정리하기 위한 논의가 지속적으로 이루어지고 있다. 논의 결과 IDMEF(Intrusion Detection Message Exchange Format)[9]와 IAP (Intrusion Alert Protocol), CIDF(Common Intrusion Detection Framework), IDXP(Intrusion Detection exchange Protocol)와 같은 표준화 방안과 데이타 변환 방안에 대하여 발표되고 있다.

IDMEF, IDXP, IAP 등의 포맷은 아직 표준화 과정이 진행 중[7]이고 모든 발생 가능한 이벤트의 범주를 포함하여 변환하기 위해서는, 아직 포맷이 복잡하기 때문에, 현재 발생하고 있는 복합적인 보안 위협(예, CodeRed, Nimda, Slammer)이나 미래에 발생할 수 있는 알려지지 않은 보안 위협을 표현하기에 부적절하며 실제적인 위협요소를 판별하기에는 어려운 점이 많이 남아 있다.

3. SIA 시스템

SIA 시스템에서는 메시지 통합을 위해 필수정보만을 얻을 수 있도록 자체의 표준 포맷을 제안하였다. SIA 로직을 이용했을 때, 멀티센서로부터의 로그를 상호연관시키고 메시지를 통합, 분석하여 직관적인 메시지로부터 상세한 위험 정보를 쉽게 인지할 수 있다. 특히, 대량의 로그 파일이 발생하는 대형기관에서는 많은 거짓 경보를 줄일 수 있으며 시스템과 네트워크 전체의 위협에 대해 쉽게 인지하고 대처방안을 세울 수 있다.

SIA 시스템의 특징은 다음과 같이 요약할 수 있다.

첫째, 멀티센서 경고 통합 모니터링 기능을 제공한다.
둘째, 네트워크상의 위협을 실시간 감시할 수 있다.
셋째, 대량의 거짓 경보를 줄일 수 있으므로 네트워크 위협판단에 필요한 인력의 낭비를 줄일 수 있다.
넷째, IDS와 Firewall의 멀티센서로부터 수집한 정보를 통해 침입자의 의도 파악 및 추적이 쉽다.

SIA 시스템에서는 멀티센서로 부터의 로그와 포맷을

최소한의 판단 조건을 지닌 데이타의 형태로 간략화 하여 데이타베이스에 저장한 후 유형 판단 로직(Status Evaluation Logic)을 적용해 정보시스템의 위협을 알려줄 수 있다. 개별적인 특정 위협 보다는 거시적인 관점으로 위협에 대해 판단할 수 있는 로직을 제공한다. 소스 IP와 목적지 IP를 기준으로 하여 공격자의 시스템에 대한 접근의도를 알아 낼 수 있도록 구성되어 있다.

3.1 IDS와 Firewall의 침입 경고 메시지 포맷 정의

표준화 되지 않은 멀티센서에서 침입분류 파악에 도움이 되는 필수적인 정보들을 얻기 위해 필요한 포맷으로 가공하였다. 간략하고 필수적인 정보만을 가지고 효과적인 위협을 탐지하는 것이 가능하도록 여러 부가 정보들은 표준 포맷에서 제외하였다. 현장에서 활용도가 높은 제품중심으로, Firewall 표준 포맷은 Cisco사의 PIX, Netscreen사의 Netscreen, Checkpoint사의 FW-1에서 추출한 데이타 포맷을 바탕으로 하여 구성하였고, 이는 다른 Firewall 제품에서도 공통적으로 발견할 수 있는 부분이므로 경고 메시지와 이벤트 처리시에 쉽게 변환이 가능한 부분이다(표 1). IDS의 표준 포맷 정의를 위해 ISS사의 ICECAP Manager, Snort, Real Secure의 포맷을 조사하여 표준 포맷을 구성하였다(표 2). 표 2에서 IDS의 표준 포맷을 볼 수 있으며 표 1, 표 2에 나타나 있는 형태를 이용하여 각 IDS와 Firewall 제품이 표시하는 경고 메시지와 이벤트에서 SIA 시스템을 구성하기 위한 표준 포맷에 해당하는 정보를 추출하였다. 즉, 모든 보안시스템은 표준 포맷을 포함하는 내용을 가지고 있는 경우에, 저수준의 경고 메시지로부터 표준 포맷의 형태의 데이타를 추출하는 전환 장치만 제작하게 되면 SIA 시스템에 바로 적용이 가능하다.

표 1 Firewall 표준 포맷

Time	yyyymmdd-HHMMSS:message receive time
Address	Sensor address
Address	Source IP address
IP Address	Destination IP address
	Detected signature
	Signature priority
	IDS raw message

표 2 IDS 표준 포맷

Receive Time	yyyymmdd-HHMMSS:message receive time
Action	Firewall Action string
Protocol	TCP/UDP
Interface	Sensor Interface
Sensor Address	Sensor IP address
Source Address	Source IP Address
Destination Address	Destination IP Address
Source Port	Source Port
Destination Port	Destination Port
Detail	Firewall raw message

3.2 침입행위 분류

침해사고 및 침입자의 의도에 대해 정보시스템 영역에서 판단하였을 경우, SIA 시스템에서는 유형 판단 로직에 따라 침입자의 공격 유형을 네 가지 형태로 요약해서 분류하고 있다. 첫 번째는 특정 대상에 대해서 많은 호스트들이 공격을 가한 경우, 두 번째는 네트워크 영역에 대한 취약점 스캐닝 및 공격, 세 번째는 정보시스템 내의 특정 목적지에 대한 공격이나 공격시도, 네 번째는 정보시스템 영역 전반에 걸친 대규모 스캔의 형태로 분류가 가능하다. 대부분의 정보보호 시스템의 경우 특정 공격에 대해서 경고 메시지와 이벤트를 발생시키는 형태로 이루어져 있으며 거짓 경고가 다수 존재하기 때문에 모든 경고에 대해 모두 대처하기 어려운 실정이다. 예를 들어서 Nimda 웜의 경우를 보면 Code-Red의 공격패턴과 Unicode 공격, CodeRed 백도어 공격이 혼재되어 있으므로 센서들이 침입을 탐지하여, 각각의 경우에 대해 통합 대응하기 어려움을 알 수 있다. 즉, CodeRed 공격인지 Unicode 공격 혹은 Nimda 공격인지 분별할 수 없다. 공격은 다양한 방법으로 세분화되고 복합화 되어가는 경향을 보이는 반면에 침입탐지 시스템은 하나의 공격에 일일이 반응하는 형태로 되어 있다. 센서들이 동일한 웜에 대해 반응하는 경고 메시지 형태는 저마다 다르며 이전의 CodeRed 공격과 중복될 뿐만 아니라 멀티센서들로부터 발생하는 경고 데이타의 양이 너무 많기 때문에 보안 관리자에게 과도한 혼란을 유발시키게 된다. 이런 실제적인 위협의 기준을 거시적인 위협형태로 분류함으로써 즉각적으로 침입위협 유형을 손쉽게 판단할 수 있도록 새로운 모델을 제안하였으며, 위협영역을 공격자 IP와 목적지 IP의 갯수를 기준으로 4가지 유형으로 분류하였다(그림 4).

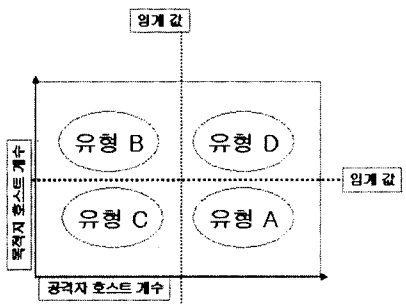


그림 4 새로운 SIA 분석 방법

임계 값(threshold value)에 따라 위험 유형의 판정 기준이 정해지는데, 이 임계 값은 네트워크 관리 시스템의 범위에 따라 달라질 수 있고 판정의 기준 값이 공격자 IP와 목적지 IP를 기준으로 하며, 이 기준 범위를 임계 값으로 정하였다. 임계 값과 목적지 호스트 개수를 이용해서 A, B, C, D 유형으로 분류 하였다. 해킹 공격 유형들을 살펴 보면 1 : n, n : n, n : 1 그리고 1 : 1의 공격 유형으로 나타나는데, 기존의 방화벽이나 침입탐지 시스템들은 이를 너무 세분화하기 때문에 신속하게 침입유형을 파악하고 즉시 대응하기 위해서는 간단명료하게 분류하기 위해서, 공격자의 숫자나 목적지 호스트의 숫자를 적절한 임계 값으로 설정하였다.

각 유형은 분산 네트워크 환경에서 공격자 호스트의 개수와 목적지 호스트의 개수에 따라 구분되어 질 수 있다. 예를 들면, 공격자 호스트의 개수가 적고 목적지 호스트의 개수가 많을 경우에는 최근 취약점에 대한 네트워크 서브넷 스캐닝으로 볼 수 있다. 4개의 유형으로 분류하는 목적은 여러 개의 센서들로부터 수집한 경고 데이타를 이용해 네트워크의 위협을 판정 하는데 있다. A, B, C, D 유형에 대한 각각의 판단 기준은 다음과 같이 설정 될 수 있다. 판단 기준의 의의는 경고 데이타를 기준으로 하여 침입을 판정하는 것이 아니라, 특정 네트워크 영역에 속해 있는 대상 자원에 대한 공격과 위협을 기준으로 하여 네트워크 영역에 대한 위협요소를 판단하는 것이 중요하다. 이런 판단을 내리는 기준 요소로서 많은 센서로 수집한 데이타로부터 침입 판정을 위해 공격자 IP 주소와 목적지 IP 주소값을 기준으로 이용하여 네트워크 영역에 대한 위험을 판단하는 요소로 사용하였으며, 네트워크 영역에 대한 각 위험 유형은 다음과 같은 형태로 정리될 수 있다.

유형 A는 멀티 호스트로부터 특정 서버로 연결이 집중되는 유형을 나타낸다. 예를 들어, 유형 A인 경우는 DDoS 공격 및 멀티 커넥션 등의 문제를 나타낸다. 유형 B는 특정 IP 대역 네트워크에 대한 스캐닝이 발생한 것을 나타낸다. 예를 들어, 유형 B인 경우에는 Net Bus, Back Orifice 2k 등과 같은 특정 포트를 사용하는 백도어에 대한 클래스대역 혹은 IP 영역에 대한 스캐닝 시도 등을 의미하게 된다. 유형 C의 경우는 특정 대상 서버에 특정 공격자의 공격이 집중된 것을 나타낸다. 즉, 유형 C는 호스트에 대한 직접적인 스캐닝 및 관련 정보 수집, 무차별 공격(Brute Force) 등의 경우를 나타낼 수 있다. 유형 D에서는 공격 메시지의 수량에 따라 일상적인 유형의 공격 로그들과 웜 공격 유형에 대해서 구분한다. 예를 들어, 유형 D인 경우는 정보시스템 영역에 대한 광범위한 스캐닝 또는 웜 공격을 의미하게 된다.

4. SIA 시스템 구현

SIA 시스템 구현은 Firewall 관련 메시지의 처리 부분과 IDS 경고 처리 부분, SIA 로직 처리부, 데이타 처리 부분으로 나누어 볼 수 있으며 전체적인 구성은 IDS와 Firewall 경고 데이타가 저장되는 부분에서 표준 포맷 형태의 메시지를 얻어낸 후 데이타베이스에 저장하는 부분과 데이타베이스에 저장된 부분을 가공하여 디스플레이하는 상위 부분으로 구분할 수 있다. 하위 부분은 Firewall 처리 부분과 IDS 처리 부분으로 나뉘어져 있다(그림 5).

구현과정에서 유형 판단 로직의 시간간격(Interval Time)을 최대 3분으로 주고 테스트 하였을 경우, 웜(Nimda, Codered)의 공격이 집중된 경우, 유형 판정값 하나와 연관되는 경고 메시지는 400개 이상인 경우도 존재하였다. SIA 로직을 이용하여 네 부분의 상호연관 관계 경고 메시지로 변환함으로써 관리 네트워크상의 위협 유형을 거시적으로 4가지 유형으로 판단하여 외부 침입을 즉각적으로 탐지하고 대응할 수 있게 된다.

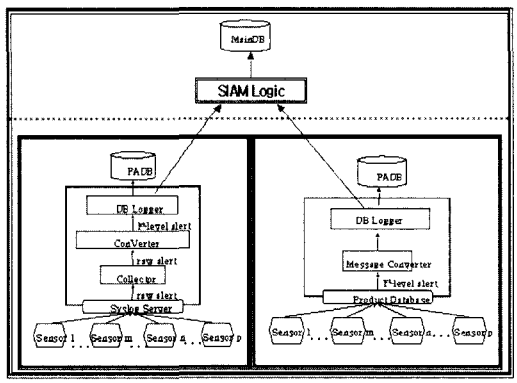


그림 5 SIA 시스템 다이어그램

4.1 SIA 시스템 구조

SIA 시스템 구조는 매니저(Manager)와 컨버터(Converter)로 구성되어 있으며, 구현 대상 멀티센서 중에서 IDS는 ISS ICECAP(BlackIce Manager) 2.6, 3.0과 Snort 1.7, Snort 1.8을 대상으로 했으며, Firewall은 PIX를 기준으로 구현하였다. 컨버터 설치용 서버로는 Pentium III 800Mhz, RAM 256MB PC 서버 두 대와 매니저용으로 Zeon Dual processor, RAM 512MB인 서버를 사용하였다. DB 서버로 MS SQL 2000과 프로그래밍 언어로 C, 개발 도구로는 Visual C++ 6, Visual Basic 6을 사용하였다. 컨버터 설치용 서버는 OS의 구분이 없으며 매니저용은 Windows 2000 서버를 사용하였다. 내부 기능의 구조는 멀티센서로부터 경고 메시지

를 받아서 처리하는 형태로 되어 있다(그림 5). Firewall의 경우에는 컨버터를 다양화 하지 않고 현재의 구현에서는 Syslog로만 한정시켰다. 컨버터에서는 Syslog로 저장된 메시지를 데이타베이스에 저장하고, 메시지를 표준 포맷 형태로 변환하였다. IDS 컨버터 디자인에서는 각 제품과 별개로 사용하는 데이타베이스가 존재하며 데이타베이스에 저장된 메시지를 읽어서 표준 포맷의 형태로 상위 단계의 데이타베이스에 저장하였다.

4.2 SIA 시스템 디자인

유형을 판별하는 유형 판단 로직 부분의 구성은 쓰레드 버퍼를 이용하여 주요 판별요소를 저장한 후, 경고 메시지에 따라 유형을 판별하도록 하였다(그림 6).

유형 판단 로직에 따른 처리와 간격 시간 값에 따른 버퍼처리 부분에는 다양한 방식이 존재할 수 있으며, 본 논문에서의 구현은 쓰레드를 활용한 버퍼를 이용하여 구현을 하였다. 유형 판단 로직의 구성은 그림 7과 같다.

Process 1은 새로운 데이타를 확인한 후 바로 제어가 넘어가는 부분이며 이곳에서의 처리는 그림 8과 같은 세부 루틴을 지니고 있다. 그림 8에 나타나 있는 Status는 각 센서로부터 수집한 정보를 상태 유형에 따라 분류하여 SIA 데이타베이스에 정보를 수집하는 과정을 의미하고 있다. Comp1에서는 새롭게 들어온 데이타에서 공격자 IP가 버퍼에 저장된 공격자 IP와 같은지의 여부를 조사한다. Comp2에서는 Comp1 절차에서 공격자 IP가 서로 같을 경우에 실행되며 여기에서는 목적지 IP와 버퍼의 목적지 IP가 같은지 비교한다. 비교하여 같으면 유형 C 절차로, 같지 않으면 유형 B 절차로 제어를 넘긴다. Comp3에서는 Comp1 절차에서 공격자 IP가 서로 다를 경우에 실행되며 즉 새로 들어온 메세지의 공격자 IP와 버퍼에 저장된 공격자 IP가 일치하는 것이 존재할 때 목적지 IP와 버퍼에 저장된 목적지 IP가 동일한지

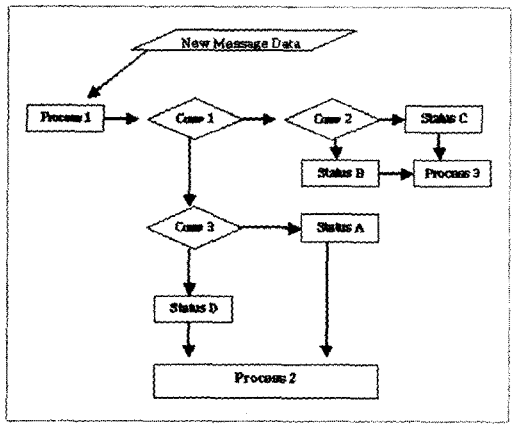


그림 7 유형 판단 로직

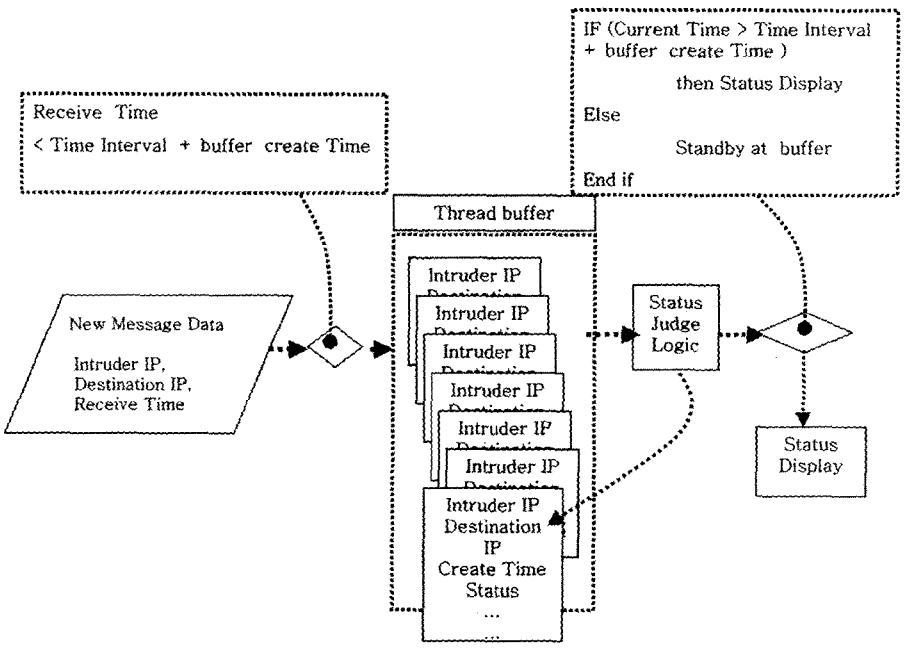


그림 6 SIA 처리부분

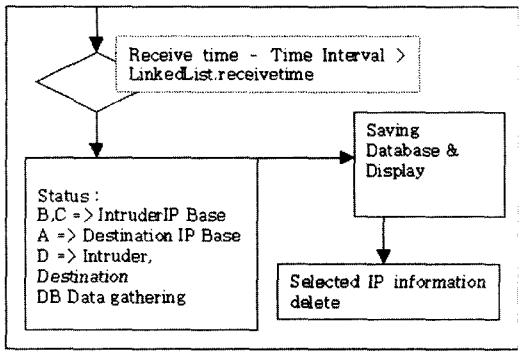


그림 8 Process 1 작업

검사한다. 만약 여기에서 목적지 IP가 같다면 유형 D로 제어를 넘기고 목적지 IP가 같지 않다면 유형 A로 제어를 넘긴다.

그림 8의 "LinkedList.receivetime"은 경고 메시지를 받았을때 자료구조에 저장되는 경고 메시지의 수신 시간을 나타내며, "Time Interval"은 ESM에서 임계값으로 지정한 기간을 의미한다. 그리고 Receive Time은 새롭게 들어오는 경고 메세지의 Receive Time을 가리킨다.

```
Update Buffer Value
Receive Time, Intruder IP, Destination IP(IP can be replaced by Hostid)
```

그림 9 Process 2 작업

Process 2에서는 현재 존재하는 버퍼에 Receive Time, Intruder IP, Destination IP, status value D 또는 A 값을 추가한다. 이 경우의 Receive Time은 공격 유형 판별로직이 완료된 후의 과정으로서 공격 유형이 판별이 되고 나면 최종 공격 유형 판정에 참고된 경고 메세지 도착 시간이 발생시간이 됨으로 최종 경고세미지t의 Receive Time을 공격 유형 판별 Receive Time으로 갱신할 때 사용되는 시간을 나타낸다. 즉, 경고메세지의 Receive Time을 공격 유형을 판별하는 최종 Receive Time으로 갱신하는 과정이다.

```
IF Intruder IP = Buffer saved Intruder IP and
IF Destination IP  = Buffer saved Destination IP  then
        Status value change → Status C
Else
        Status value change → Status B
END IF
```

그림 10 Process 3 작업

Process 3에서의 처리 로직은 다음과 같다. Process 3에서는 공격자 IP와 저장된 공격자 IP가 같고 목적지 IP와 저장된 목적지 IP가 같을 경우 유형 값을 D 또는 A에서 C로 변경한다, 그리고 목적지 IP와 저장된 목적지 IP가 같지 않을 경우 D 또는 A에서 유형 값을 B로 변경한다. 이렇게 변경된 유형 값을 버퍼에 업데이트 시키게 된다. 판단 조건의 유형 값에 따른 분기 로직을 정리해 보면 다음과 같다. 그림 11에서 "If Receive Time > Buffer -> ReceiveTime + Time Interval" 코드는 수신시간이 일정시간을 경과한 이후에는 특정한 시간간격 이후 버퍼에 저장되어 있는 자료들을 갱신하여 새로이 판단하도록 자료를 갱신하는 과정을 나타내고 있다.

```
IF Receive Time > Buffer -> ReceiveTime + Time Interval
    If status B, C then
            Buffer.IntruderIP = IntruderIP
    Else if A then
            Buffe.DestinationIP = DestinationIP
    Else

            Buffer.DestinationIP =DestinationIP &
              Buffer.IntruderIP = IntruderIP
  END IF
Else
            Buffer Clear
END IF
```

그림 11 유형판단 분기 로직에 대한 Pseudo 코드

각 컨버터를 거친 데이타들이 중간 단계를 거쳐서 상위 DB로 전달되는 과정을 도식화하면 그림 12와 같이 표현될 수 있다.

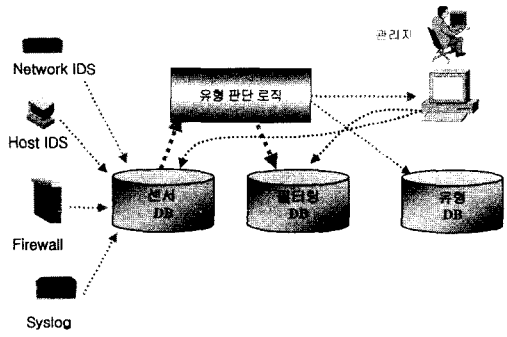


그림 12 로그 데이타 흐름도

유형 판단 부분에서 SIA 로직이 적용되며 판단에 해당되는 데이타는 중간 단계의 필터 DB에 저장이 된다. 최종 SIA 로직에 의해 해당 유형이 판정이 되면 최종 판정의 정보를 유형 DB에 입력하고 유형 판정에 관련된 데이타를 필터 DB에 입력하는 구조로 되어 있다.

엔터프라이즈 환경에서의 다양한 판별기준과 환경을 고려하여 이 프로그램에서 구현한 기능은 다음과 같이 요약할 수 있다.

1) SIA 로직을 이용하여 침입 경고를 간략화 한다.

2) 침입자별 침입 유형을 분류해 준다.

3) 기본적인 MAE(Meta Analysis Engine) 기능을 수행하고 IDS와 Firewall의 로그를 상호연관시킨다.

4) 각 센서별 로그에 대한 상세 침입 정보를 확인해 주는 기능을 제공한다(IDS는 모두 지원, Firewall은 PIX 지원).

4.3 SIA 경고 시스템(Alert System)

SIA 로직을 적용하게 되면 유형 값이 나열되며 각 유형을 더블클릭하게 되면 유형 판정의 값이 나오며, 판정값을 선택할 경우 특정 침입자가 남긴 Firewall과 IDS의 전체 로그를 확인할 수 있다. 유형 값을 더블클릭 하면 메인 화면으로 전환되며 상단에는 필터링된 메시지가 나타나고 필터링된 메시지를 선택할 경우, 하단에 IDS와 Firewall의 경고 메시지가 나타난다.

또한 도구 화면에 출력된 경고 메시지를 선택할 경우, SIA 시스템에서는 Ping, Whois, Trace route, Visual route, Port scan과 같은 기능을 사용할 수 있도록 제공하고 있다. 그림 14는 유형 구분의 기준이 되는 임계 값은 3으로, 버퍼에 저장된 결과를 재설정 하는 시간 간격은 3 분으로 고정하여 테스트한 결과를 보여주고 있다. 실험은 24시간을 기준으로 1시간 단위의 경고 메시지를 체크 하는 형태로 이루어 졌고 시간 영역(Time Zone)은 GMT+9로 설정하였다. 그림 14는 실제 IDS의 경고 메시지와 SIA 로직이 적용되어 발생되는 경고 메시지 수의 비율을 보여주고 있다. 실제 IDS에서 발생한 경고 메시지 수와 SIA 로직이 적용된 후의 유형 발생 비를 보면, 경고 메시지 발생 개수에 따라 SIA 경고메시지가 증감 하는 것을 알 수 있다.

각 유형별 발생 빈도는 그림 15에 나타나 있다. 각 유형별 그래프가 다른 이유는 네트워크 침입 유형에 따른 것으로 테스트 결과는 2003년 1월을 기준으로 하였다. 침입 탐지 센서를 기준으로 테스트된 결과로서 주된 침입패턴은 CodeRed 웜, Nimda 웜, 웹 서버 백도어 공격, 스캐닝 등이 다수 존재 했으며 웜의 영향으로 인해 임계 값에 따른 특정 유형 값이 다수 발생하였다. 유형

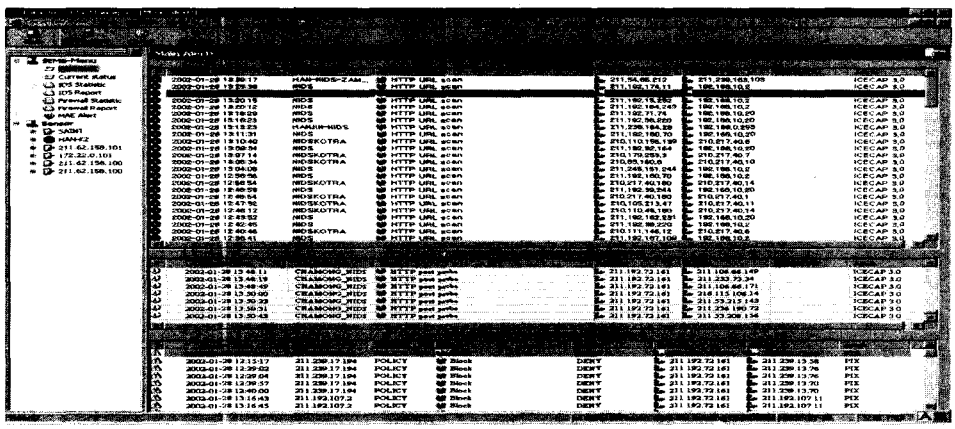


그림 13 SIA 시스템 유형 경고 데이터

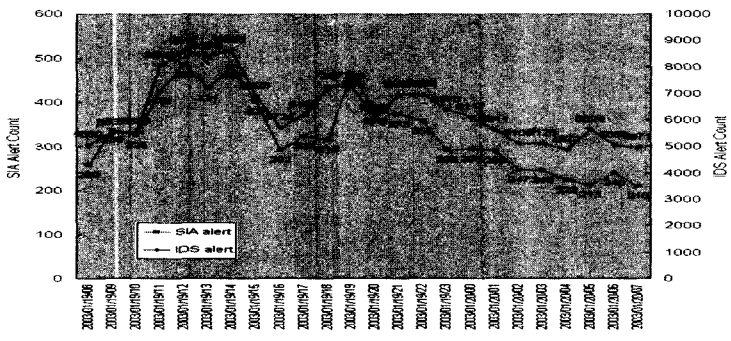


그림 14 IDS 경고 데이타와 SIA 경고 데이타 비교

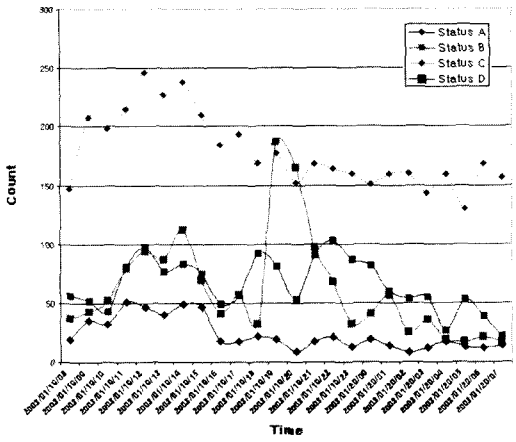


그림 15 유형 값에 따른 메시지 개수 그래프

C의 개수가 지속적으로 높게 나온 것은 Nimda 웜의 영향과 임계 값이 낮게 책정됨으로써 전체적인 유형 개수보다 높은 비율을 유지하고 있다. Nimda 웜의 특성은 랜덤하게 공격 대상 IP를 선정한 후 공격대상에 대해 24가지 이상의 웹 서버 공격루틴을 이용하여 공격을 수행하고 다음 공격대상으로 옮겨가는 형태를 반복한다. 단일 서버에 대한 집중적인 공격의 형태가 이루어지고 있어서 유형 C의 개수가 높게 나오는 원인이 됨을 알 수 있다. Nimda 웜에 대한 대책이 완료되었을 경우에는 임계 값을 조정하여 알려지진 않은 공격을 탐지할 수 있도록 조정할 수 있다. 그림 15에서 유형 B의 급격한 변화는 일시적으로 다량의 스캐닝이 이루어졌으며, 분석 결과 백도어의 존재를 확인하는 패턴 및 연결을 시도하는 공격이 다수 존재하였다. PC에 저장된 백도어를 통한 연결 시도와 백도어의 존재 여부를 확인하기 위한 스캐닝이 이루어지는 것을 확인할 수 있었다. 유형 발생 빈도에 영향을 미치는 요인으로는 임계 값과 시간간격이 존재하며 현재 SIA 시스템을 구성한 환경에서 나타나는 요인별 유형 개수를 확인하여 임계 값과 시간간격 값을 구성환경에 맞추어 변경할 경우 최적의 결과를 얻을 수 있다. 유형 발생요인 별 유형 개수의 변화는 발생되는 공격패턴 및 웜 공격방식에 따라 변경이 될 수 있다. 즉 센서가 설치된 네트워크 영역의 특성과 서버의 보안 수준, 웜의 활동 등에 의해 유형별 발생빈도는 달라질 수 있으며 발생 패턴의 경우도 달라질 수 있다.

각 유형의 임계 값 및 시간 간격에 따라 유형 개수가 달라지게 된다. 그림 16에서 임계값을 3으로 설정한 이유는 테스트 환경에서 유형 판별로직의 변별력을 높이기 위해서 이다. 가장 Alert이 많이 발생되었던 Nimda와 Codered 웜의 경우 전파 비율이 같은 서브넷 상에서는 60 퍼센트 정도이고 다른 클래스 대역에 대해서는 40 퍼센트의 비율로 공격이 이루어 졌고 10회 이상의 공격이 짧은 시간에 집중이 되는 현상이 계속 이루어져서 웜의 정확한 판단이 중첩이 되는 경우가 다수 생하였다. 즉 단일 서버에 대한 여러 공격자들의 집중적인 공격과 웜에 의해 일정비율로 공격이 이루어지는 상태에 대해 유형 값의 혼선이 이루어져서 테스트 환경에서는 두 비율을 구분할 수 있는 상태가 임계값 3이었고 Interval Time이 3분인 상태였다. 임계값을 3 미만으로 설정할 경우 Nimda와 Codered 웜에 의해 특정 서버에 이루어지는 10여회의 공격 시도가 빠른 주기로 반복이 이루어짐으로 인해 웜에 대한 판별과 다수의 서버에서 이루어지는 Scan 공격의 구분이 어렵다. 임계값을 4 이상으로 설정하였을 경우 테스트 환경에서는 웜에 의한 공격이 이루어짐에도 불구하고 다수의 서버에서 이루어지는 스캔 공격으로 판별하는 문제점들이 존재하였다.

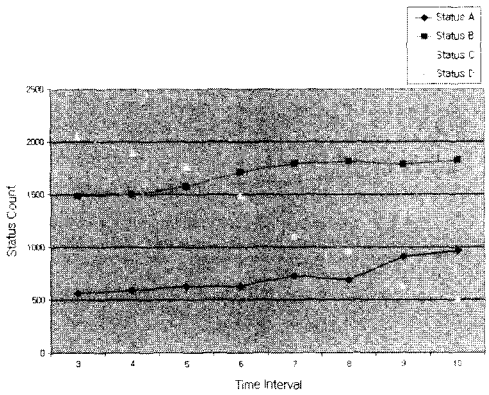


그림 16 시간 간격에 따른 유형 변화(임계 값 3으로 고정)

본 논문의 테스트 환경에서 나타나는 유형 값은 보안 대책을 세워 줄여 나갈 수 있다. 즉, 많이 발생하는 유형에 대해서 충분한 보안 대책을 적용한 후에는, 임계 값 및 시간 간격을 적절히 조절함으로써 새로운 공격 패턴이나 침입유형을 판단할 수 있는 유형을 유지하게 할 수 있다. 임계 값 및 시간 간격을 조정함으로써 과다 발생하는 유형에 대해 조정을 할 수 있으며 조정하는 이유는 다음과 같다. 알려진 취약점을 통해 일상적으로 일어나고 있는 해킹에 대해 대책이 마련되어 있고 각 서버 단위에서의 보안 대책이 구성되었을 경우 중요 값을 조정하여 특정 유형을 과다 발생시키는 원인을 줄여줌으로써 유형 발생 분포를 통한 새로운 형태의 침입유형을 판별하는 데 도움을 줄 수 있다. 본 논문의 환경에서는 유형 C의 과다 발생 원인인 Nimda 웜에 대한 보안 대책을 센서가 설치된 네트워크 영역에 대해 시행한 뒤라면 임계 값 및 시간 간격의 조정을 통해 충분히 낮

추게 되면 새로운 침입유형이나 이상증세의 발견을 쉽게 할 수 있다.

5. 결 론

새롭게 발생하는 침입과 위협은 단일 공격이 아닌 웜에 의한 무작위 공격 및 특정 서버를 목표로 하는 DDoS 공격이 점차 증가하고 있다. 이처럼 복합된 공격 형태를 지니고 있어서 관리 네트워크상의 위협을 판단하고 조치를 취하는 것이 어렵다. 이에 따라, 숙련된 전문가 인력을 통해 오랜 시간동안 수집한 로그파일을 분석해야하는 해당 보안 위협을 판단 할 수 있는 제한점을 갖고 있다. 즉 현재까지의 위험요소를 판정하는 부분은 복합화된 공격에 취약하며 관리 네트워크 영역에 대한 거시적인 위협판단이 어려울 수 밖에 없다. 본 논문에서는 각 센서에서 수집한 많은 로그 정보들을 필수적인 표준 포맷 형식으로 변환하여 관리 네트워크 영역에 공격을 가하는 공격자와 대상에 대한 값을 이용하여 해당 위협요소를 판정할 수 있도록 하였다. 또한 멀티센서를 운용하는 관리 네트워크 상에서 발생하는 대량의 경고 메시지를 간략화 함으로써 휴먼 리소스의 의존을 줄일 수 있으며 위협에 대한 관점을 개별 경고 메시지 분석 수준에서 관리 네트워크 영역 전체에 대한 위험수준을 판정할 수 있도록 함으로써, 복잡화 되어가고 조직화 되어가는 공격에 대응할 수 있는 시스템을 운용할 수 있도록 하였다. 향후 연구 방향으로는 관리 네트워크 영역에 대한 위협 요소를 세분화 하고, SIA 시스템의 성능을 개선하고, SIA 시스템을 통해 발견된 경고 메시지를 통해 해당 보안 위험에 자동적으로 대처하는 방안을 연구하고자 한다.

참 고 문 헌

[1] P. Ning, Y. Cui, D. S. Reeves, "Construction Attack Scenarios through Correlation of Intrusion Alerts," ACM1-58113-612-9, pp. 245-254, 2002.

[2] M. Botha, R. V. Solms, K. Perry, E. Loubser and G. Yamoyany, "The Utilization of Artificial Intelligence in a Hybrid Intrusion Detection System," Proceedings of SAICSIT 2002, pp. 149-155, 2002.

[3] P. Ning, "Abstraction-Based Intrusion Detection In Distributed Environments," ACM Transactions on Information and System Security, Vol.4, No.4, pp. 407-452, 2001.

[4] T. Bass, "Intrusion Detection Systems And Multisensor Data Fusion," Communications of the ACM, Vol.43, No.4, pp. 99-105, 2001.

[5] D. Frincke, "Balancing Cooperation and Risk in Intrusion Detection," ACM Transactions on Information and System Security, Vol.3, No.1, pp. 1-29, 2000.

[6] NetForensics Article, http://www.netforensics.com, 2003.

[7] P. Loshin, Information Security Magazine article for Meta-IDS, http://www.infosecuritymag.com/articles/june01/columns_standards_watch.shtml, 2001.

[8] IDMEF XML Library (libidmef) Version 0.6.1 API 2002, Silicon Defense. http://www.silicondefense.com/idwg/libidmef/API, 2002.

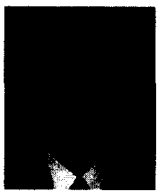
[9] D. Curry, Intrusion Detection Message Exchange Format Extensible Markup Language(XML) Document Type Definition, http://www.ietf.org/ids.by.wg/idwg.html, 2003.

한 근 희

1982년~1996년 KIST 시스템공학연구소 연구원. 1986년~1988년 한양대학교 산업대학원 석사(전산학전공). 1996년~2000년 데이콤 인터넷사업본부 부장/팀장. 2000년~2002년 (주)한시큐어 대표이사 사장. 2000년~2003년 고려대학교 대학원 컴퓨터학과 박사 수료. 2002년~현재 (주)엠디엠아이앤씨 부사장. 2003년~현재 건국대학교 정보통신대학원 겸임교수. 관심분야는 ESM, 인터넷 보안, 모바일 보안, 차세대 인터넷

전 상 훈

1992년~2000년 울산대학교 산업공학과 졸업. 1998년~2000년 (주)신성정보기술 개발팀장. 2000년~2000년 A3 Security consulting consultant. 2000년~2002년 한시큐어 기술연구소 연구원. 2002년~2002년 넷시큐어 선임 컨설턴트. 2002년~현재 SK infosec 전임 컨설턴트. 관심분야는 ESM, 인터넷 보안, 모바일 보안, 보안 컨설팅



김 일 곤

2000년 경기대학교 영어영문학과 졸업 2002년 고려대학교 컴퓨터학과 석사 졸업. 2003년 고려대학교 컴퓨터학과 박사과정 수료. 관심분야는 정형기법, 소프트웨어 공학, 보안 프로토콜, 보안 운영체제

최 진 영

1982년 서울대학교 컴퓨터공학과 졸업 1986년 Drexel University Dept. of Mathematics and Computer Science 석사. 1993년 University of Pennsylvania Dept. of Computer and Information Science 박사. 1993년~1996년 Research Associate, University of Pennsylvania. 1996년~1999년 고려대학교 컴퓨터학과 조교수. 1999년~현재 고려대학교 컴퓨터학과 부교수. 관심분야는 컴퓨터이론, 정형기법(정형 명세, Formal verification), 실시간 시스템, 분산 프로그래밍 언어, 소프트웨어 공학