지식기반 실시간 사이버위협 조기 예·경보시스템

이동휘* · 이상호* · 김귀남*

요 약

최근 사이버테러의 급증은 정보사회의 근간을 위협하고 있고, 특히 악성 트래픽에 의한 네트워크 마비는 단 시간 내에 국가적인 손실을 초래할 수 있어 이에 대한 대비책이 시급히 요구되고 있다. 이와 관련, 국가사이버안전 위협에 대한 신속한 대처능력확보를 위해 국가사이버위협 조기 예·경보시스템에 대해 많은 연구가 이루어지고 있으나, 기술적인 문제와 함께 시스템의 효용성에 대한 한계 때문에 실용적인 연구가 가시화되지 못하고 있는 실정이다. 현재까지는 ESM, TMS등을 이용한 제한적 자료수집분석을 통하여 보안관리자가 개개인의 경험을 바탕으로 예·경보 판단을 내려왔다. 이러한 판단은 상황에 따라 극히 위험한 결과를 초래 할 수도 있다. 이러한 문제점을 방지하기 위해 본 논문에서는 "지식기반을 이용한 실시간 사이버위협 조기 예·경보시스템"을 제안하였다. 제안된 시스템은 향후 사이버공격에 대해 체계적이고 보다 정확한 예·경보 판단을 내리는데 사용할 수 있다.

A Conceptual Design of Knowledge-based Real-time Cyber-threat Early Warning System

Dong-Hwi Lee* · Sang-Ho Lee* · Kuinam J. Kim*

ABSTRACT

The exponential increase of malicious and criminal activities in cyber space is posing serious threat which could destabilize the foundation of modern information society. In particular, unexpected network paralysis or break-down created by the spread of malicious traffic could cause confusion and disorder in a nationwide scale, and unless effective countermeasures against such unexpected attacks are formulated in time, this could develop into a catastrophic condition. As a result, there has been vigorous effort and search to develop a functional state-level cyber-threat early-warning system : however, the efforts have not yielded satisfying results or created plausible alternatives to date, due to the insufficiency of the existing system and technical difficulties. The existing cyber-threat forecasting and early-warning depend on the individual experience and ability of security manager whose decision is based on the limited security data collected from ESM (Enterprise Security Management) and TMS (Threat Management System). Consequently, this could result in a disastrous warning failure against a variety of unknown and unpredictable attacks. It is, therefore, the aim of this research to offer a conceptual design for "Knowledge-based Real-Time Cyber-Threat Early-Warning System" in order to counter increasing threat of malicious and criminal activities in cyber space, and promote further academic researches into developing a comprehensive real-time cyber-threat early-warning system to counter a variety of potential present and future cyber-attacks.

Key words : Cyber-threat, Early Warning System

* 경기대학교 정보보호학과

1. 서 론

21C 인터넷 기반 산업의 활성화는 엄청난 경제적 가치를 창출하고 있으나, 정보화의 역기능인 컴퓨터 바이러스 유포, 악의적 해킹 및 사이버테러의 급증은 정보사회의 근간을 위협하고 있어 이에 대한 대비책이 시급히 요구되고 있다. 특히 최근 주요 이슈로 부각되고 있는 악성트래픽에 의한 네트워크 마비, 전자상거래 방해 등과 같이 단시간 내에 엄청난 국가적 손실을 초래할 수 있는 악성 웜, 바이러스, 해킹 등 다양한 사이버위협 요소에 대한 신속한 대처능력의 확보는 보안관리업무에 있어 매우 중요한 요소로 부각되고 있다. 이런 국가적 위협에 대응할 수 있는 가장 근본적인 대책은 사이버 공격에 미리 대처 할 수 있는 조기 예·경보시스템을 구축하는 것이라고 할 수 있다.

지금까지의 조기경보는 대부분 트래픽 분석 의존기법(traffic-based analysis technique)이 주종을 이루어왔다.

Hellerstein(2001)이 트래픽의 조기경보를 위해 Seasonal ARIMA모형을 적용하여 기간망(wired-network)의 주간 트래픽 양을 예측한 것이 그 사례이다[1]. 또한 F. Zang(2000)은 Seasonal ARIMA 모형을 활용하여 무선통신의 트래픽을 예측하였고[2], Groschwitz(1994)는 웨이블릿 분석을 사용하여 원래의 트래픽을 각각의 시간 주기에 따라 분해하여 각각의 필터링된 신호를 통해 트래픽 상황에 대한 장기적인 이상과 단기적인 이상을 쉽게 구분하는 방법을 제시하였다[3]. Y. Shu는 퍼지-자기회기모형(Fuzzy-AR model)으로 비선형적이고 비정류적인 고속 네트워크 트래픽을 예측하는데 적합한 방법을 제시하였다[4]. Hellerstein, F. Zang, and Y. Shu 등이 사용한 기법들의 가장 큰 공통점은 대규모 트래픽 양이 폭주하는 상황 및 이상징후발생에 대해 임계치 분석기법에 의한 상황예측이 가능한 모델을 제시하였다는 점이다. 그러나 최근 트래픽 폭주 유발위협의 특성이 단순한 포트공격, 또는 순차적인 공격이 아닌 인공지능적인 기법과 불규칙 공격속도에 따른 확산공격방법으로 진화하고 있기 때문에[5] 트래픽을 계량적으로만 판별한 방법에 의존한 분석기법으로는 최근 사이버위협에 대한 예측이 어려울 수 밖에 없다.

C. Zou(2003)는 Kalman Filter 예측기법을 사용하여 유행성 웜 모형의 관측자료를 통한 모니터링 기법으로 인터넷 웜 감시 및 조기경보를 가능케 하는 기술을 연구하였다[6]. 그러나 이는 표본추출에 의존한 연구로서 2가지 이상의 취약성을 이용하거나 자체. 인공지능기능을 통한 불규칙 확산 웜의 경우 위협검출이 어렵다는 단점이 있다.

J. B. D. Cabrera(2003)의 SNMP 기반의 트래픽의 MIB변수를 활용한 DDoS 조기 탐지기법에 관한 연구[7]와 J. Zhai(2003)의 Dempster-Shafer 증거이론을 활용하여 네트워크 침해를 조기에 경보하는 기법[8], J. Li(2003)의 단일 MIB변수를 대상으로 통계적 분석을 수행하여 DoS공격을 조기에 탐지하는 기법연구[9] 역시 사이버위협을 조기 예·경보 하기 위한 기법으로 활발히 연구되어 왔으나, 이들 기법은 DoS공격이라는 특정 위협에 대한 경보만 가능하여 체계적인 조기 예·경보 시스템으로 진화하기에는 많은 제약이 있다는 단점이 있다.

문호건(2005)은 사이버 취약점과 위협의 상관성 분석을 통한 네트워크 위험 및 취약점 상관연구[10] 에서 N-IDS와 VAS의 상관 분석을 통해 사이버위협 예측이 가능하였다. 문호건(2005)이 제시한 분석모델을 통한 사이버 위협 예측 및 예·경보는 N-IDS가 탐지할 수 없는 취약성과 변종에 대한 접근방식이 최근 사이버위협패턴임을 고려할 때 제한적일 수 밖에 없는 한계를 가지고 있다.

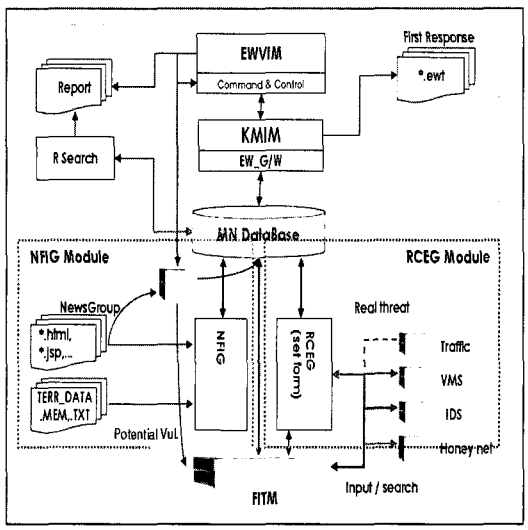
2. 지식기반 실시간 사이버 조기 예·경보시스템

사이버위협에 대한 대응의 가장 중요한 요소는

공격에 대한 조기탐지 및 이에 따른 분석기법 그리고 각 대응기법 및 메커니즘이 유기적으로 연계되도록 하는 통합된 조기 예·경보시스템의 설계라 할 수 있다.

2.1 조기 예·경보 위협관리시스템 (EWTMS : Early Warning and Threat Management System) 설계

(그림 2-1)은 EWTMS의 전체 구성도를 나타낸다. (그림 2-1)에서와 같이 EWTMS는 4개의 모듈로 구성된다. 이벤트 데이터 수입의 기능은 NFIG(News Find Input Gateway), RCEG(Real Critical Event Gateway), 그리고 FITM(First Input Threat Module) 모듈이 수행된다.



(그림 2-1) EWTMS 구성도

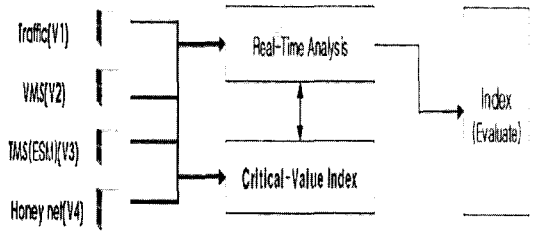
NFIG, RCEG, 그리고 FITM은 본 제안 시스템의 구성요소로 새로이 제안된 모듈로서 NFIG는 실시간 사이버위협정보를 수집하여 정형화하며, RCEG는 각 보안장비 이벤트를 수집하고, FITM은 각 보안장비에서 탐지하지 못한 변종 및 취약성 위협에 대해 수집하는 것을 말한다.

각 데이터 수집 모듈은 각기 다른 성격의 데이터를 수집하여 (그림 2-1)의 MN DataBase로 수집된 정보를 전송한다.

DataBase로 모아진 정보는 다시 KMIM (Knowledge Management Integration Module)에서 분석되고, 분석된 결과는 EWVIM (Early Warning Visual Information Module)으로 보내져 report와 함께 다양한 그래프 화면으로 나타난다.

각각의 모듈은 다음과 같은 기능을 가진다.

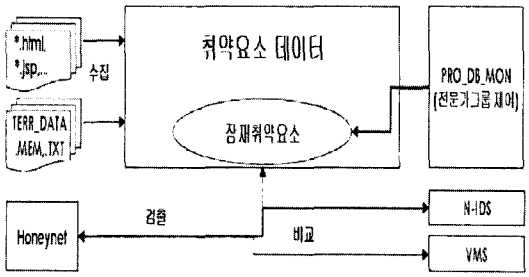
2.1.1 RCEG(Real Critical Event Gateway)



(그림 2-2) RCEG 구성 및 동작구조

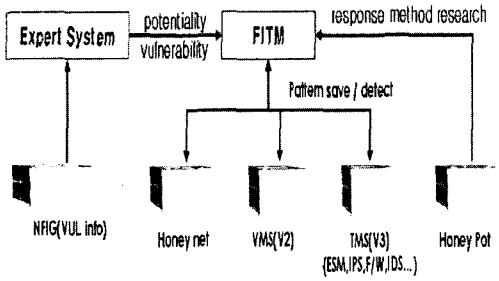
RCEG의 구성과 동작구조는 (그림 2-2)와 같다. RCEG는 내부 네트워크의 위협 정도를 평가하기 위해 대표적인 4가지 보안장비 이벤트를 실시간으로 입력 받아(real-time input) 각 단위 별 임계치(level of critical value)를 설정하고 정형화하여 KMIM으로 전송한다.

2.1.2 FITM(First Input Threat Module)



(그림 2-3) FITM 구성 및 동작구조

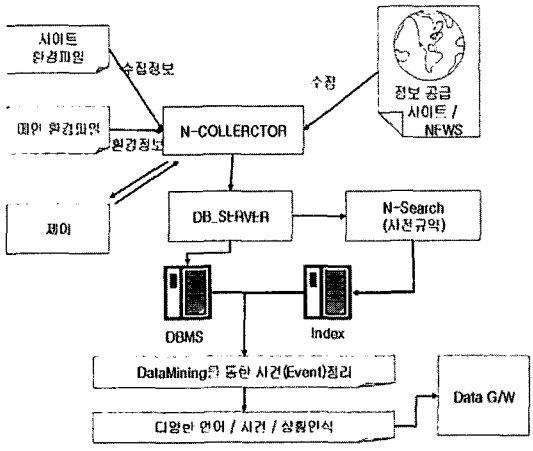
FITM의 구성과 동작구조는 (그림 2-3)과 같다. FITM은 NFIG에서 취약요소 데이터를 수집하고, 각 보안장비에서 탐지하지 못한 사이버 위협요소에 대해서는 Honeynet을 통해 수집한다. 수집한 정보는 각 보안장비의 이벤트 패턴과 비교 분석하여 잠재취약요소를 판단한다.



(그림 2-4) FITM 주변 구성도 및 동작구조

FITM의 주변 구성도와 동작구조는 (그림 2-4)와 같다. NFIG로부터는 취약성정보를 수집하고, Honeynet및 각종 보안장비를 통해서는 패턴을 검출하여 잠재 사이버위협요소의 확산방법을 분석하기 위해 MN DataBase로 보내어지게 된다.

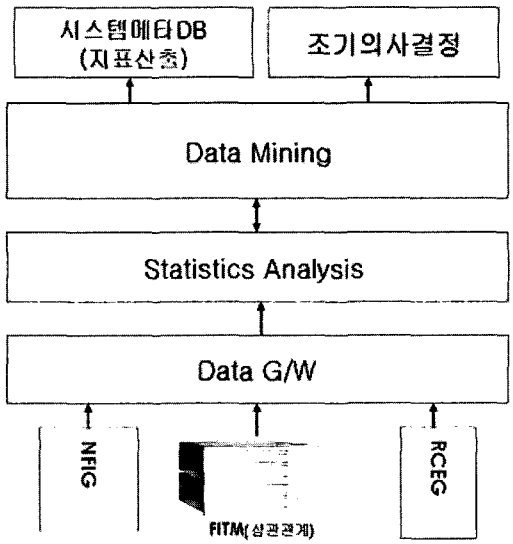
2.1.3 NFIG(News Find Input Gateway)



(그림 2-5) NFIG 구성도 및 동작구조

NFIG의 구성과 동작구조는 (그림 2-5)와 같다. NFIG는 실시간 사이버위협정보를 자동으로 입력받아 D/B를 구축하고 이D/B에서 사이버 위협 관련 정보만 추출하여 이를 기반으로 사이버 위협을 판단한다. 이렇게 판단된 정보는 NFIG와 RCEG의 상호 보완을 통하여 조기에 위협동향을 파악하게 된다.

2.1.4 KMIM(Knowledge Management Integration Module)



(그림 2-6) KMIM 구성도 및 동작구조

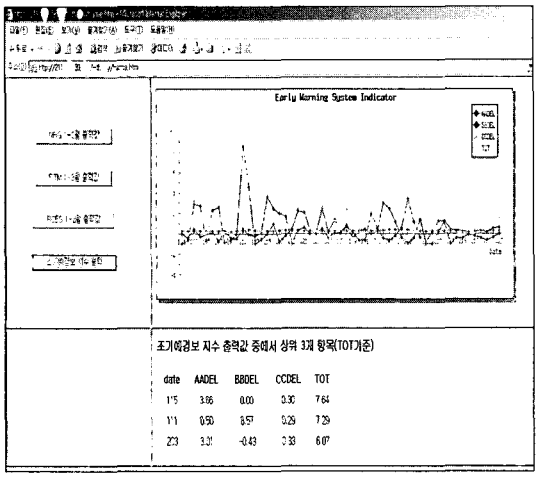
KMIM의 구성과 동작구조는 (그림 2-6)과 같다. KMIM은 3가지 데이터 입력 모듈에서 가져온 정보를 분석하여 조기 예·경보지수를 산출하게 된다. 먼저 FITM에서 내부 네트워크에서 잠재취약요소 검출을 통한 값을 산출한다. 이렇게 검출된 값은 NFIG의 취약요소 매칭을 통하여 누적된 상관관계 값을 산출하고, NFIG에서 정형화된 이벤트 값 과 마지막으로 RCEG에서 보안장비 이벤트데이터는 표준화를 통한 수치 값을 산출한다.

위에서 산출된 정보를 통계분석기법과 지식관리기법을 이용한 분석값을 분류기법을 통하여 지

표를 설정하고 평가한다. 동 분류기법은 개체 또는 사건을 서로 다른 속성을 가지도록 분리하고 할당하는 분류기법을 통해 그룹화한다. 분류기법의 궁극적인 목적은 문제의 목적과 적합한 결과를 산출하여 사이버위협 조기 예·경보 판단 담당관의 판단과 유사한 의사결정을 할 수 있는 모형을 구축하는 것이다.

2.1.5 EWVIM(Early Warning Visual Information Module)

EWTMS 메인 시스템에서는 제어를 통한 지표 산출 값과 조기의사결정 Data를 가지고 최종결과를 (그림 2-7)과 같이 그래프와 수치로 도출한다.



(그림 2-7) EWVIM Display

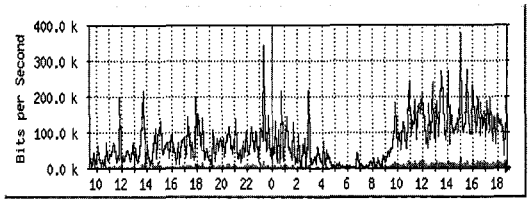
3. 제안 시스템 검증 및 분석

3.1 각 요소 별 이벤트데이터 정형화 분석

3.1.1 Traffic 부분

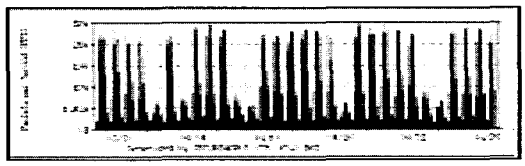
가) 각 백본망(back-bone network) 트래픽에 대한 5분 단위 평균값을 기준으로 하여 생성된 그래프

일간 그래프 (5 분 단위 평균값 기준)

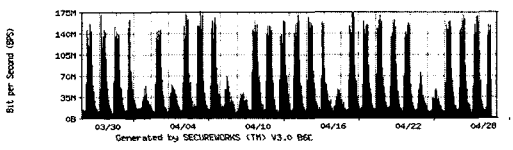


최대 수신: 29.8 kb/s (0.3%) 평균 수신:7936.0 b/s (0.1%) 현재 수신: 22.1 kb/s (0.2%)
최대 송신:374.9 kb/s (3.7%) 평균 송신: 72.3 kb/s (0.7%) 현재 송신:281.0 kb/s (2.8%)

(그림 3-1) 트래픽 일간그래프



(그림 3-2) 패킷량 그래프

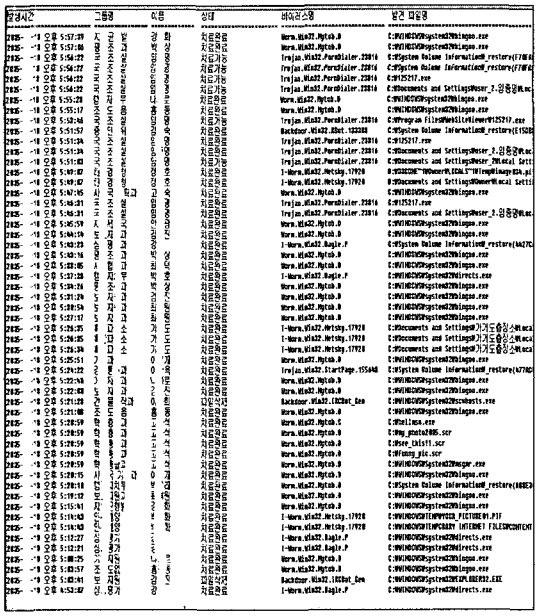


(그림 3-3) 데이터량 그래프

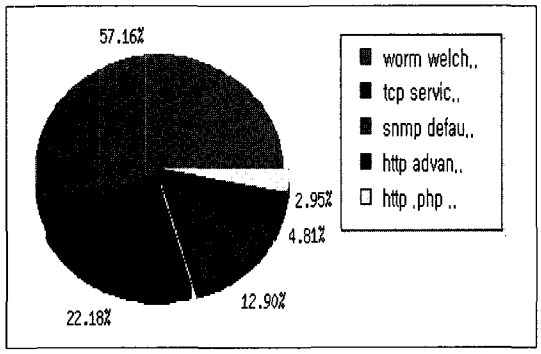
(그림 3-1)은 A기관의 트래픽 일간(daily) 그래프를 보여주고 있으며, (그림 3-2)는 A기관의 주간 패킷량(packet volume) 그래프, (그림 3-3)은 A기관의 주간 데이터량 그래프를 보여주고 있다. A기관의 네트워크 트래픽 양에 대한 입력 값을 다양하게 EWTMS에 적용하였다.

3.1.2 VMS외 이벤트 적용 프로세스 임계치 설정을 위한 데이터 수집과 정규화

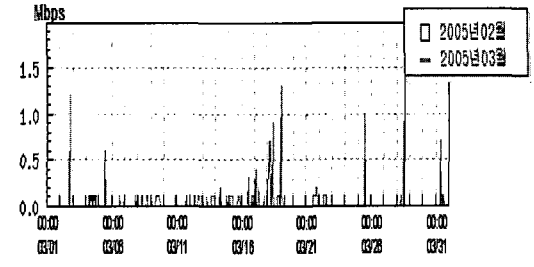
(그림 3-4)는 A기관의 VMS 시간별 데이터를 나타내고 있으며, 실험에 사용된 데이터는 VMS 실제 데이터로서 VMS의 시간별 데이터, 그룹별 데이터, 일간, 월간데이터의 변수를 추출하여 임계치를 구성하였다.



(그림 3-4) VMS 시간별 데이터



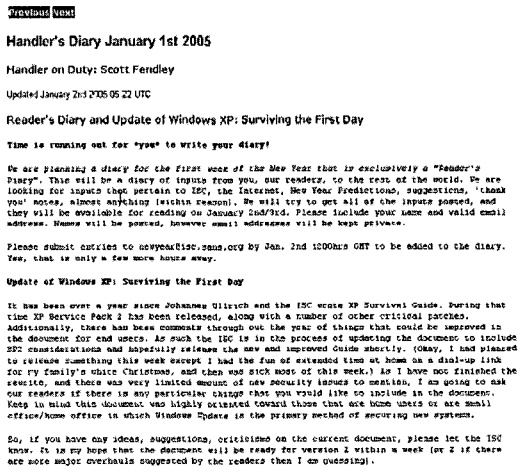
(그림 3-5) 일일 공격형태 분포내역



(그림 3-6) 전월 대비 유해 트래픽 추이

(그림 3-5)는 일간 공격형태 분포내역을 나타내고 있고, (그림 3-6)은 월간 유해 트래픽을 지난달과 대비시킨 추이를 나타내고 있다. 이렇게 수집된 보안장비 이벤트 데이터를 일간, 시간별, 월간 데이터로 나누어서, 각 데이터는 모델의 임계치 통계를 위한 데이터 집합(Data Set)으로, 임계치 모델(critical value model)의 테스트를 위한 테스트데이터 집합(Test Data Set)으로, 실제 실시간 데이터는 분석모델의 평가를 위한 평가데이터 집합(Evaluation Data Set)으로 사용하였다.

3.1.3 News Data Input



Previous Next

Handler's Diary January 1st 2005

Handler on Duty: Scott Fendley

Updated January 2nd 2005 05:22 UTC

Reader's Diary and Update of Windows XP: Surviving the First Day

Time is running out for *you* to write your diary!

We are planning a diary for the first week of the New Year that is exclusively a "Reader's Diary". This will be a diary of inputs from you, our readers, to the rest of the world. We are looking for inputs that pertain to ISC, the Internet, New Year Predictions, suggestions, 'thank you' notes, almost anything (within reason). We will try to get all of the inputs posted, and they will be available for reading on January 2nd/3rd. Please include your name and valid email address. Names will be posted, however email addresses will be kept private.

Please submit entries to newyear@isc.sans.org by Jan. 2nd 1200hrs GMT to be added to the diary. Yes, that is only a few more hours away.

Update of Windows XP: Surviving the First Day

It has been over a year since Johannes Ullrich and the ISC wrote XP Survival Guide. During that time XP Service Pack 2 has been released, along with a number of other critical patches. Additionally, there has been comments through out the year of things that could be improved in the document for end users. As such the ISC is in the process of updating the document to include SP2 considerations and hopefully release the new and improved Guide shortly. (Okay, I had planned to release something this week except I had the fun of extended time at home on a dial-up link for my family's white Christmas, and then was sick most of this week.) As I have not finished the rewrite, and there was very limited amount of new security issues to mention, I am going to ask our readers if there is any particular things that you would like to include in the document. Keep in mind this document was highly oriented toward those that are home users or are small office/home office in which Windows Update is the primary method of securing new systems.

So, if you have any ideas, suggestions, criticisms on the current document, please let the ISC know. It is my hope that the document will be ready for version 2 within a week (or 2 if there are more major overhauls suggested by the readers then I am guessing!).

(그림 3-7) NFIG는 사이버위협정보를 자동으로 입력 받아 DataBase로 입력하는 것을 나타내고 있다. NFIG의 동작구조는 추출하려는 원천 데이터 소스 제공처를 선정하여 이가 제공하는 데이터의 입력 형태를 분석한다. 이를 토대로 하여 NFIG에서 입력시킬 수 있는 텍스트 모드로 각각의 데이터들을 전환한다. 전환된 데이터를 빈도분석(frequency analysis)과 시계열분석(time series analysis), 회귀분석(regression analysis) 기법 등을 사용하여 수치화 하고 수치화된 데이터는 가중치요소를 첨가하여 KMIM으로 보내지게 된다.

- ** -
Updated January 2nd 2005 05 : 22 UTC
This will be a diary of inputs from you, our readers, to the rest of the world.
please include your name and valid email address.
however email addresses will be kept private.

Updated January 4th 2005 19 : 23 UTC
Those include, but not limited to
I was looking for the global trend pattern int the port traffic after the 0 day!
I knew security was one of my weakerareas, and so I made the SANS ISC my ahead of the malware coming at my systems from so many vectors.
- ** -

(그림 3-7) News 관련 Database 입력

3.2 성능분석 모델

3.2.1 조기 예·경보시스템 구성을 위한 실험 조건

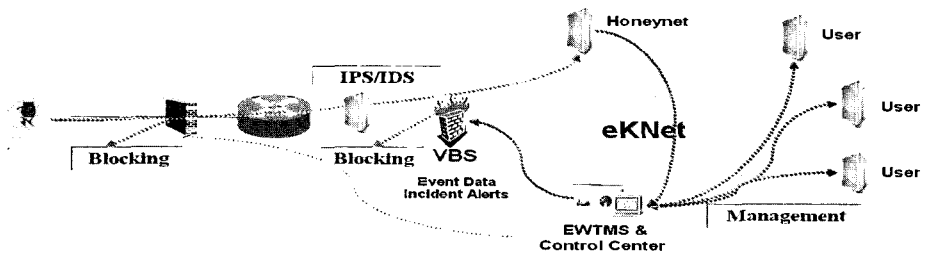
한 달간 1G Byte속도 이상을 사용하고 외부망(external network)과 내부망(internal network)이 분리되어 있으며, 내부망의 경우 가상(virtual)IP를 사용하는 대형 네트워크(이하 A 네트워크)에 (그림 3-8)과 같은 조건의 보안장비를 적용하여 실험하였다. 먼저 IPS(Intrusion Prevention Systems)와 TMS가 백본구간(Backbone section)에 설치되어 있고 백본구간에는 허니넷 시스템을 사용하여 내·외부망에 대한 정보를 측정하였다. VMS는 메인 시스템에서 클라이언트로 각 말단 PC에 설치되어 있다. A네트워크에서는 EWTMS를 이용한 시스템을 구성하였고, 지난 90일간의 데이터로 장비별 임계치를 적용하여 실험하였다. 보안장비로는 VMS(Virus Management System), F/W(Firewall), IDS, IPS, TMS 등이 동일하게 구성되었다.

3.2.2 이벤트 데이터의 적용

사이버위협 조기 예·경보시스템을 검증하기 위해 과거데이터를 EWTMS에 적용하여 2005년 1월부터 2005년 3월까지의 결과값(result)을 도출하기로 했다. 사이버위협 예보상황 도출은 A네트워크에서 내부 및 외부 트래픽양(또는 방화벽)의 순간 점유율(share) 70%가 1분 이상 지속되는 것으로 잠정 결론을 내렸다. 잠정수치는 A네트워크 자체적으로 네트워크가 정상작동하지 못하는 수치를 임계화하여 내린 결론이다.

3.3 실험 결과

NFIG에서는 2005년 1월부터 3월까지 12개의 원천데이터로부터 입력 값을 받아 DB에 저장한 후 패턴인식기법을 이용하여 위협데이터를 분류, 다시 데이터마이닝 기법으로 수치화 시킨 뒤 적용된 결과값은 <표 3-1>과 (그림 3-9) 이하 그래프로 다음과 같이 생성되었다.



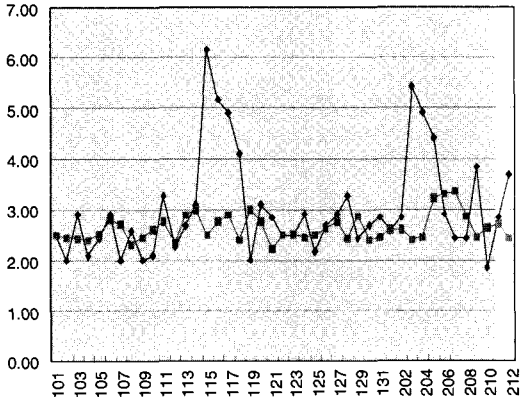
(그림 3-8) 실험구성도

〈표 3-1〉 NFIG 위협데이터 분포

	분포					
	1	2	3	4	5	6
표준화(A1)	9162	05	1.91998	-.65107	1.06297	1.91998
표준화(A2)	0000	36	83666	-1.67332	3.34664	.00000
표준화(A3)	5106	- 2708	1.13733	-.80335	1.13733	2.68988
표준화(A4)	3 4449	-. 5590	-.08677	-.45990	.65948	-.45990
표준화(A5)	-1 4606	828	1. 78262	-.30317	3.34696	-.30317
표준화(A6)	- 1129	-495	3.99067	-.11129	.57237	-.11129
표준화(A7)	3596	-1 6606	-. 43735	-.43735	.28596	.28596
표준화(A8)	- 5515	-2 7921	-1. 39650	1.56891	.08620	.08620
표준화(A9)	-1 3453	-2 5197	-1. 03709	.63522	.63522	.63522
표준화(A10)	4. 3057	-8526	2.16798	-1.26656	.69604	-.28526
표준화(A11)	3. 3907	-6661	1.56623	-.46232	.34910	-.6232
표준화(A12)	1. 436	-2703	2.56092	-.92703	-.42875	56781
표준화(Total)	2 0599	-10258	2.35140	-.92078	1.86057	1.04253
표준화(Avl)	2 0689	-10224	2.35209	-92377	1.86169	1.03782
표준화(Avl,old)	6627	7724	-.86783	-.10549	.96179	-.86783
표준화(A1)	49162	0595	1.91998	-65107	1.06297	1.91998
표준화(A2)	00000	3666	-.83666	-1.67332	3.34664	.00000
표준화(A3)	36106	2708	1.13733.	-.80335	1.13733	2.68988
표준화(A4)	64449	5590	-0.8677	-.45990	.65948	-.45990
표준화(A5)	-1 4606	1828	1.78262	-.30317	3.34696	-.30317
표준화(A6)	-. 129	9495	3.99067	-.11129	.57237	-.11129
표준화(A7)	. 596	-1 6066	-.43735	-.43735	.28596	.28596
표준화(A8)	-. 515	-2 7921	-1.39650	1.56891	308620	.08620
표준화(A9)	-1 453	-2 5197	-1.03709	63522	.63522	.63522
표준화(A10)	4 8057	8526	2.16798	-1.26656	.69604	-.28526
표준화(A11)	8907	5661	1.56623	-4.6232	.34910	-.46232
표준화(A12)	6436	2703	2.56092	-.91703	-.42875	356781
표준화(Total)	0599	- 00258	2.35140	-92078	1.86057	1.04253
표준화(Avl)	0689	00224	2.35209	-.92377	1.86169	1.03782
표준화(Avl,old)	6627	67724	-86783	-.10549	.96179	-.86783

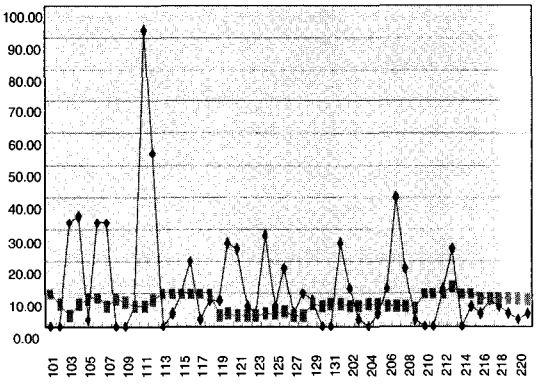
		표준화(A1)	표준화(A2)	표준화(A3)	표준화(A4)	표준화(A5)	표준화(A6)	표준화(A7)	표준화(A8)	표준화(A9)	표준화(A10)
상관계수	표준화(A1)	1 00	20	.270	.082	-.053	.228	-.016	-.124	.097	.140
	표준화(A2)	20	1 00	.425	.230	.509	.368	-.029	-.192	.011	.274
	표준화(A3)	70	25	1.000	.367	.213	.439	.162	-.114	-.008	.441
	표준화(A4)	32	80	.367	1.000	-.036	.361	.045	-.144	.032	.781
	표준화(A5)	- 53	09	.213	-.036	1.000	.415	.017	.054	-.059	.039
	표준화(A6)	28	68	.439	.361	.415	1.000	.056	-.135	.000	.535
	표준화(A7)	- 16	29	.162	.045	.017	.056	1.000	.166	.016	.041
	표준화(A8)	24	32	-.114	-.144	.054	-.135	.166	1.000	.278	-.148
	표준화(A9)	97	11	-.008	.032	-.059	.000	.016	.278	1.000	-.166
	표준화(A10)	40	74	.441	.781	.039	.535	.041	-.148	-1.66	1.000
	표준화(A11)	09	8	.418	.723	-0.78	.344	-.011	-.016	.053	.789
	표준화(A12)	24	98	.237	.289	.127	.389	-.123	-.085	-.138	.492
	표준화(Total)	36	2	.697	.697	.289	.671	.164	0.11	.165	.772
	표준화(Avl)	36	12	.697	.698	.289	.672	.164	0.10	.164	.772
	표준화(Avl,old)	52	40	.054	.004	.039	-.117	.107	-0.37	-.090	-.043
	표준화(A1)	1 00	20	.270	.082	.-053	.228	-.016	-.124	.097	.140
	표준화(A2)	20	1 00	.425	.230	.509	.368	-.029	-.192	.011	.274
	표준화(A3)	70	25	1.000	.367	.213	439	.162	-.114	-.008	.441
	표준화(A4)	-82	30	.367	1.000	-.036	361	.045	-.144	.032	.781
	표준화(A5)	-53	09	.213	-.036	1.000	415	.017	.054	-.059	.039
	표준화(A6)	28	68	.439	.361	.415	1.000	.056	-.135	.000	.535
	표준화(A7)	-16	29	.162	.045	.017	.056	1.000	.166	.016	.041
	표준화(A8)	-24	- 32	-.114	-.144	.054	-.135	166	1.000	.278	-.148
	표준화(A9)	17	11	-.008	.032	-.059	.000	016	.278	1.000	-.166
	표준화(A10)	0	74	.441	.781	039	.535	.041	-.148	-.166	1.000
	표준화(A11)	19	18	.418	.723	-.078	.344	-.011	-.016	0.53	.789
	표준화(A12)	24	98	.237	.289	.127	.389	-.123	-.085	-.138	.492
	표준화(Total)	36	12	.697	.697	.289	.671	.164	.011	.165	.772
	표준화(Avl)	36	12	.697	.698	.289	.672	.164	.010	.164	.772
	표준화(Avl,old)	-. 82	40	.054	.004	.039	-.117	.107	-.037	-.090	-.043

a. 행렬식 = .000
b. 이 행렬은 양의 유한값이 아닙니다



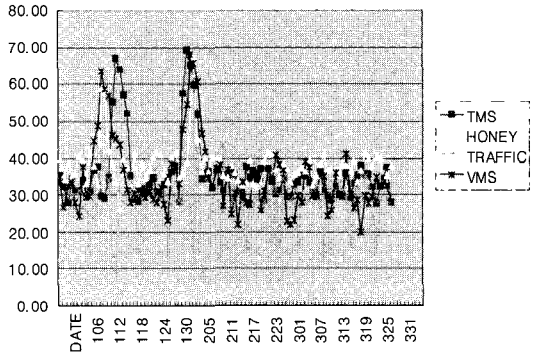
(그림 3-9) NFIG 1~3월 출력값

(그림 3-9)의 결과치를 보면 분홍색 임계치 라인에 비하여 115~119, 202~206에서 높은 수치를 보이고 있다.

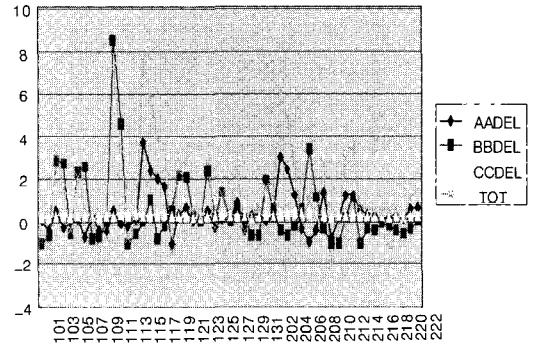


(그림 3-10) FITM 1~3월 출력값

(그림 3-10)의 NFIG 값 가운데 취약성 정보를 추출하여 대입시킨 데이터를 보면 X좌표의 111~114, 121, 202, 208에서 수치가 높다는 것을 확인할 수 있다. 특히 (그림 3-10)의 111에 나타난 취약점은 FITM에서 잠재취약성으로 분류되어 있는 데이터로서 익스플로잇(exploit)이 발표된 정보이다. 그 결과, (그림 3-9)를 보면 115에서 영향을 미쳤다는 것을 알 수 있다.



(그림 3-11) RCEG 1~3월 출력값



(그림 3-12) 조기예경보 지수 출력

(그림 3-12)는 최종 결과값을 그래프로 도출한 결과 화면이다. 결과값을 보면 1월 11일, 15일, 2월 3일 3회에 걸쳐 사이버 위협에 대한 조기 예·경보를 발령하는 것이 가능한 것으로 나타나 있다. 이런 결과가 도출된 이유는 NFIG에서 MS05-001과 MS05-002 MS05-003등 모든 취약점이 발견되었고, FITM 잠재 취약요소에 의한 공격이 강하게 나타나고 있기 때문이다. (그림 3-11)를 검토해보면 1월 15일경부터 사이버위협요소 수치가 높아진 것을 알 수 있으며, A네트워크 대응보고서에서도 1월 15일경 변종 bot 공격으로 인하여 내부 네트워크에 트래픽 이상 증상을 보였다는 보고가 있다. 그리고 트래픽 위험 잠정수치에 약 4회 접근하였다. 따라서 본 논문에서 제안한 사이버위협

조기 예·경보시스템이 4일전에 가동되어 적시성 있는 경보가 발령되고 그에 따른 대응방안을 강구하여 사전에 대처했다면 결과적으로 트래픽이 폭주하거나, 내부 네트워크의 위협요소를 차단 할 수 있었을 것이라 판단된다.

4. 결 론

4.1 실험의 한계

실험결과 다음과 같은 한계가 발견되었다. 첫 번째 1월 15일의 예·경보지수가 높게 나타나지만 AA, BB, CC 지수가 낮게 나타나는 것으로 분석되었다. 그 결과 1월 15일 예·경보가 아닌 당일 실시간 이상 트래픽에 대해서 반응한 것으로 판단된다. 두 번째 A네트워크에서 2월 15일 대규모 MSN 메신저 공격이 있었으나 NFIG 모듈에서만 탐지 하여 2월 12일 예·경보 지수가 낮게 형성되었다. FITM에서 메신저 취약점에 대한 대비가 없었기 때문이다. 차후 메신저 취약점 및 다양한 공격루트에 대한 고려가 있다면 충분히 탐지가 가능하다고 판단된다.

4.2 향후 연구과제

최근 미국을 비롯한 많은 국가들이 사이버 위기상황을 사전에 인지하고 신속하게 대처하기 위한 다양한 위기관리 방안을 강구하고 있는 시점에서, 우리 한국 역시 여타 국가들이 시도하지 않았던 독자적인 방법으로 긴박한 사이버위기상황에 적절하게 대응하고, 위기관리차원에서 사이버안보를 강화시킬 수 있는 대안으로 지식기반 실시간 사이버위협 조기 예·경보시스템을 설계, 제시하였다. 사이버위협이 가지는 다면성과 다양한 공격에 대한 신속한 식별 및 조기판단과 대응을 가능케 해주는 이 시스템은, 이벤트데이터를 활용한 자동정보분석프로그램과 함께 위험분석 및 대안분석의 기능을 가진 지식관리기법 모델이 활용되었다. 비록 현재로서는 그 기능이 제한적이기는 하지만 사이버위기관리를 위한 기반체계의 구축이 가능하다는 결론에 도달했다. 비록 본 연구가 기초적인 수준의 조기 예·경보시스템의 구현에 그쳤지만 이후 이를 바탕으로 각종 보안 정보와 이벤트를 정형화하기 위한 데이터를 수집하여 국가보안 데이터웨어 하우스(Data warehouse)를 마련, 국가사이버위협 조기 예·경보시스템을 구축한다면 운용경험이 축적됨에 따라 보다 신뢰성 높은 사이버위협 조기 예·경보시스템으로 진화하게 될 것으로 확신한다.

참 고 문 헌

[1] J. L Hellerstein, F. Zhang, and P. Shahabuddin, "A statistical approach to predictive detection", Computer Networks, Vol. 35, pp. 77-95, 2001.

[2] F. Zang and J. L Hellerstein, "An Approach to On-line Predictive Detection", In Preoceedings Of 8th International Symposium on Modeling. ASCTS, 2000.

[3] N .K Groschwitz and G. C. Polyzos, A Time Series Model of Long-Term NAFNET Backbone Traffic, In proceedings of IEEE International Conference on Communications, 1994.

[4] Y. Shu, M. Yu, and J Liu,"Wireless traffic modeling and prediction using seasonal ARIMA models", In proceedings of IEEE International Conference on Communications, Vol. 3, 2003.

[5] http://info.ahnlab.com/ahnlab/report_view.jsp?num=416

[6] C. Zou, L. Gao, W. Gong, and D. Towsley, "Monitoring and Early Warning for Internet

Worms", In Proceedings of the 10th ACM Conference on Computer and Communication Security, pp. 10, 2003.

[7] J. B. D. Cabrera, L. Lewis, X. Qin, C. Gutierrez, W. Lee, and R. K. Mehra. "Proactive Intrusion Detection and SNMP based security management", In proceedings of IFIP/IEEE Eighth International Symposium on Integrated Net Work Managemen, pp. 225-254, 2003.

[8] J. Zhai, J. Tian, R. Du, and J. Huang, "Network Intrusion Early Warning Model Based on D-S Evidence Theory", In Proceedings of 2003 International Conference on Machine Learning and Cybernetics, Vol. 4, pp. 1972-1977, 2003.

[9] J. Li, C. Manikopoulos, Early statistical anomaly intrusion detection of DOS attacks using MIB traffic parameters, Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, pp. 53-59, 2003.

[10] 문호건, 최진기, 강유, 이명수, "취약점과 위협의 상관성 분석을 통한 네트워크 위험 조기 경보 시스템 설계", 정보보호학회지, pp. 23-32, 2005.

[11] http://isc.sans.org/alldiaries.php?month=3&year=2005, 2005.

[12] A기관, "2005년 2월 정보보호 대응 보고서", 2005.

이 동 휘

2000년 경기대학교 전자계산학과 (이학사)
2003년 경기대학교 정보보호기술공학과(공학석사)
2004년~현재 경기대학교 정보보호학과 박사과정

이 상 호

미국 세인트존스대학교 국제학과 학사
연세대학교 정치학과 석사
영국 런던대학교 킹스칼리지 전략학과 박사
현재 경기대학교 정보보호학과 대우교수

김 귀 남

미국 캔자스대학 수학과 (응용수학사)
미국 콜로라도주립대학 통계학과 (통계학석사)
미국 콜로라도주립대학 기계·산업공학과(기계·산업공학박사)
현재 경기대학교 정보보호기술공학과 주임교수