허니넷 기반의 사이버위협 조기탐지기법 연구

이동휘* · 이상호* · 김귀남*

요 약

최근 사회적인 이슈인 악성 트래픽 인한 네트워크 마비, 전자거래 방해 등과 같이 단시간내에 엄청난 국가적인 손실이 될수 있는 악성 웜, 바이러스에 대한 대처 능력은 보안관리에 매우 중요한 요소임은 자명하다. 이와 관련, 사이버위협에 대한 신속한 대처능력을 확보하기 위해 조기예·경보시스템에 대한 많은 연구가 이루어지고 있으나, 기술적인 문제와 함께 시스템의 효용성이 대한 한계 때문에 실용적인 연구가 가시화되지 못하고 있는 실정이다. 본 논문에서는 위와 같은 문제를 해결하기 위하여 대형네트워크에서 기존 보안장비에 의한 검출과는 별도로 사이버위협 조기예경보만을 위한 조기탐지기법에 대해서 연구하였다. 실제 대형네트워크에서 허니넷(Honeynet)기반의 모듈을 적용한 사이버예경보시스템을 설계하여 대형 네트워크에서 본 모듈이 악성 트래픽에 대해 얼마나 효과적으로 대처 할수 있는지에 대해 연구하였다.

A Study about Early Detection Techniques of Cyber Threats Based Honey-Net

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. In order to solve a same problem, this paper researched early detection techniques for only early warning of cyber threats with separate way the detection due to and existing security equipment from the large network. It researched the cyber example alert system which applies the module of based honeynet from the actual large network and this technique against the malignant traffic how many probably it will be able to dispose effectively from large network.

Key words : Honeynet, Network Security, Early Warning System

* 경기대학교 정보보호학과

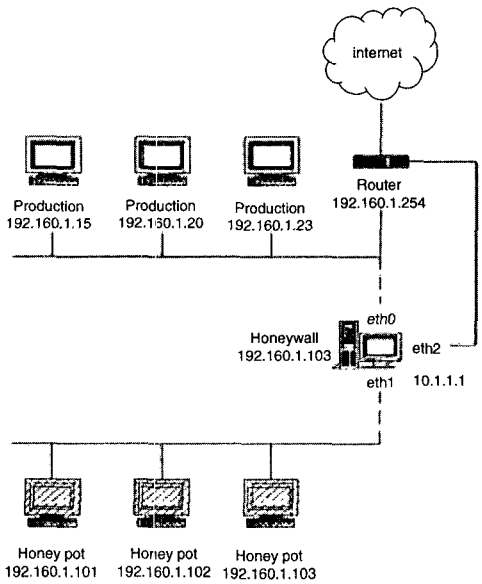
1. 서 론

유비쿼터스 환경으로 진입하고 있는 21C 네트워킹의 활성화는 엄청난 경제적 가치를 창출하고 있다. 그러나 이러한 정보화의 역기능인 컴퓨터 바이러스, 악의적 해킹 등 사이버테러의 급증은 정보사회의 근간을 위협하고 있어 이에 대한 대비책이 시급히 요구되고 있다. 특히 최근 사회적인 이슈인 악성 트래픽 인한 네트워크 마비, 전자거래 방해 등과 같이 단시간내에 엄청난 국가적인 손실이 될수있는 악성 웜, 바이러스에 대한 대처 능력은 보안관리에 매우 중요한 요소임은 자명하다.

생물학적 바이러스나 웜은 자연 발생적이지만 컴퓨터 바이러스나 웜은 대부분 제작자가 인위적으로 개선한다는 차이점이 있다. 그 차이점은 사이버위협에 대한 조기탐지가 어렵다는것과 기존의 연구되었던 논문들의 한계를 나타내고 있으며 그 한계는 사이버테러 조기예경보시스템이 실용화 되지 못하고 있는 한계를 보이는 실정이다[1]. 이러한 한계를 극복하기 위해서 조기탐지기법에 대한 필요성이 중요하게 나타나므로 본 논문에서는 허니넷기반의 예·경보시스템(Early Alert System)을 설계하여 효율적 대처가 이루어지게 함으로써 정보보호 관리자의 관리 효율과 신뢰성을 확보할 수 있도록 한다. 최근 바이러스의 경향은 자동화, 분산화, 지능화로 단시간에 광범위한 분야에 대규모 피해 유발 억제보안관리기관의 인력, 기술능력의 부족 및 독자적인 정보보호시스템 운영으로 보안사고에 어려움을 주고 있다.

2. 관련 연구

허니 시스템은 시스템을 공격하거나 침입하는 해커에 대한 정보를 수집하기 위해 제작된 허위 서버들이나 시스템들이다[2]. 허니 시스템이란 해커에 의해 공격 당함으로써 그 가치를 발휘하는 시스템을 의미하는 것으로 단지, 공격자의 정보를 수집하고 이를 이용하여 보안 강화에 도움이 될 수 있는 정보를 제공하는 시스템을 의미하는 것이다. 허니팟 시스템은 꿀단지를 의미하는 허니팟(honey pot)이라는 명칭에서도 알 수 있듯이 누군가를 유인하는 목적으로 사용된다[3, 4]. 허니넷, 허니팟 관련연구는 대부분 악성 웜바이러스 행동양식 파악하여 대처하는 방법으로 쓰여졌다. 특히 허니넷은 대형네트워크에 사용될 때 악성 트래픽에 대해서 발견 하는데 효과적이다[5].



(그림 1) 허니넷 시스템 구성도[5]

<표 1>은 취약점 공고날짜와 실제위협발생일간의 관계를 보여주고 있다. 실제로인터넷 사용자를 공포에 질리게 하는 대부분의 웜은 수 차례의 해킹을 통해 성능을 확인 받고, 짧게는 수 주 길게는 십 수개월의 잠복기를 거치면서 유포되는 악성 코드로서 관련 정보를 사전에 파악하고 있을 경우 대응이 가능하다는 사실을 인지해야 할 것이다.

〈표 1〉 취약점 관리 : 패치공고와 공격날짜의 관계[6]

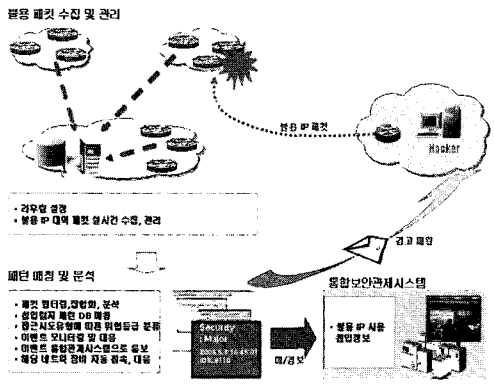
웹 이름	운영체제	관련취약점	공고날짜	공격날짜	공고와 공격날의 시간
Ramen 웜	리눅스	ftp, lprng, rpc, statd	1999-10, 2000-12	2001-01	1
LiOn 웜	유닉스 리눅스	Bind	2001-01	2001-03	2
Carko 웜	솔라리스	솔라리스 snmpXmid	2001-04-03	2001-04-19	0.5
Sadmin/IIS	솔라리스 윈도우	솔라리스 Sadmin IIS Unicode	1999-12, 2001-10	2001-05	7
Cheese웜	윈도우	LiOn backdoor	2001-01	2001-05	4
Rde 웜	리눅스	Bind, LPRng	2001-01, 2000-12	2001-06	6
CodeRed 웜	윈도우	MS01-033	2001-06-18	2001-07-13	1
CodeBlue 웜	윈도우	MS00-78	2000-10-17	2001-09	11
Nimda 웜	윈도우	MS00-78 MS01-020,ETC	2000-10-17, 2001-03-29	2001-09-18	6
Slammer 웜 Sapphire	윈도우	MS02-039	2002-07-24	2003-01-24	6

사이버 취약점과 위협의 상관성 분석을 통한 네트워크 위험 및 취약점 상관(correlation)연구[7]에서 N-IDS와 VAS의 상관 분석을 통해 사이버 위협에 예측이 가능하였다. 위 논문이 제시한 분석모델을 통한 사이버 위협 예측 및 예·경보는 N-IDS(Network Intrusion Detection System)가 탐지할 수 없는 취약성과 변종에 대한 접근방식이 최근 사이버위협패턴임을 고려할 때 제한적일 수 밖에 없는 한계를 가지고 있다.

3. 허니넷 기반의 실시간 사이버위협 조기탐지시스템 설계

3.1 허니넷 기반의 조기탐지시스템 설계

본 논문에서는 이중망을 사용하는 대형네트워크에서 사이버위협을 조기탐지할수 있는 허니넷 기반의 FITM(First Input Threat Module)을 구현하였다.



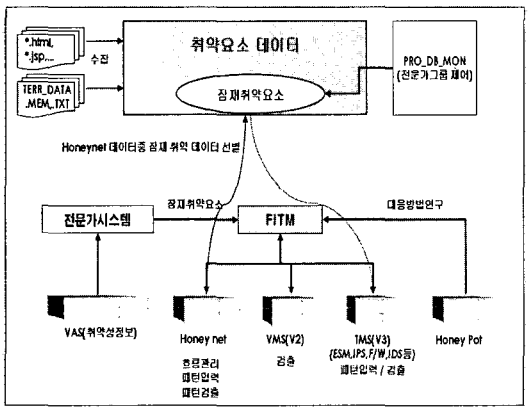
(그림 2) FITM의 기술요소

(그림 2)는 FITM의 기술요소를 나타내고 있다. (그림 2)의 처리 프로세스는 불용패킷 수집 및 관리를 위하여 라우팅 설정 및 불용IP대역 패킷을 실시간 수집 관리 엔진 설치 한다.

패턴 매칭 및 분석을 위해 패킷 필터링, 집합화, 분석을 하고 침입탐지 패턴DB 매칭 및 접근시도유형에 따른 위험등급 분류하고, 이벤트 모니

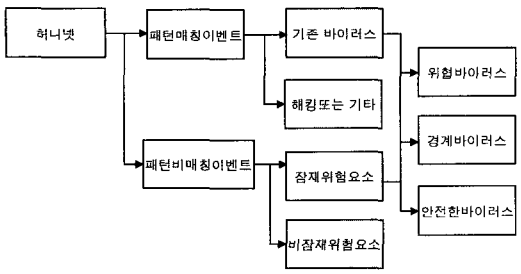
터링 및 대응에 따른 통합관제 시스템으로 통보 해당 네트워크 장비로 자동 접속 및 대응 하는 프로세스로 설계 하였다.

3.2 FITM 주변 구성도 및 동작구조



(그림 3) FITM 주변 구성도

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



(그림 4) FITM 패턴 매칭 동작구조

(그림 4)는 허니넷에서 검출된 이벤트에 대해 패턴매칭에 대한 분류 방법을 보여주고 있다. 기존 보안장비의 패턴 매칭방식과 차별화 되는 방법으로 1차 패턴매칭에대한 검출과 2차로 패턴비매칭이벤트에 대해 악성트래픽을 유발하는 잠재위협요소의 검출하여 등급을 결정 조기 탐지 기능을 갖게 하는 구조이다.

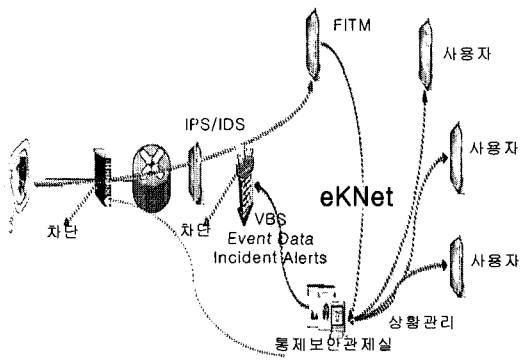
4. 성능 평가

4.1 실험환경

한달간 1G Byte속도 이상 사용하는 2개의 대형 네트워크에 같은 조건의 보안장비를 적용하여 실험 하였다. (그림 5)과 같이 A네트워크에서는 허니넷기반의 FITM을 구성하였고, B네트워크에서는 FITM을 제외하고 동일한 구성을 하였다

A네트워크에서는 FITM 분석결과를 이용하여 보안장비 룰 적용 및 예경보를 메일과 사내망을 통하여 사이버위협 예경보 정보를 게시하였다. 보안장비로는 VMS, F/W, IDS, IPS 등이 동일 구성되었다.

3개월간 VMS통계를 통한 검증 방법으로 성능평가를 하였다. A, B네트워크 10, 11월간은 FITM을 적용하지 않은 통계를 산출 하였고, 12월에는 A네트워크에 FITM 적용하여 통계를 검출 하였다.



(그림 5) FITM 적용 A네트워크 구성도

4.2 실험결과

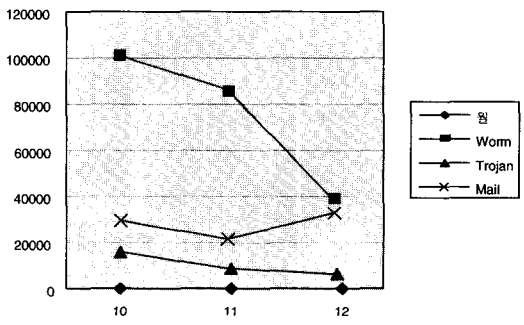
<표 2>, <표 3>의 실험결과 10 ,11월 평균은 비슷한 추이를 보이고 12월 FITM을 이용한 A네트워크가 B네트워크보다 50%이상의 웜바이러스 수가 감소한것을 알수 있다. (그림 6), (그림 7)의 그래프에서 A네트워크는 11월에 대비하여 50%이상 감소하였으나 B네트워크에서도 20%정도 감소하였으므로 A네트워크가 약 30% 정도가 더 감소했다고 추정 할수 있다.

〈표 2〉 A 네트워크 바이러스 감염수치

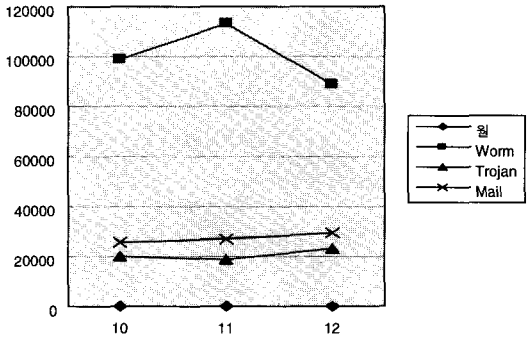
월	10	11	12
Worm	100,846	86,121	38,424
Trojan	16,355	8,532	6,722
Mail	29,412	21,990	32,455
합계	**146,613**	**116,643**	**77,601**
전달대비	100%	80%	·52%

〈표 3〉 B 네트워크 바이러스 감염수치

월	10	11	12
Worm	98,549	112,872	88,542
Trojan	20,125	18,442	23,249
Mail	25,419	26,772	29,112
합계	**144,093**	**158,086**	**140,903**
전달대비	100%	110%	89%



(그림 6) A네트워크 바이러스 그래프



(그림 7) B네트워크 바이러스 그래프

A네트워크에서 트래픽과 감염을 유발시키는 웜의 차단이 백도어성 바이러스의 감소와 비례하는 것으로 나타나고 있다.

특히 특정한 패턴을 가지고 악성트래픽을 발생시키는 worm에 대해서 효과적인 예경보가 바이러스 발생을 감소시킨다는 것을 알 수 있다.

5. 결론 및 향후과제

허니넷을 기반으로 한 FITM의 구현을 통해 미리 대처하고, 신속히 분석할 수 있는 방안에 대해 이 연구를 통하여 실험 하였다. 실험 결과 악성트래픽을 유발하는 웜바이러스에 특성을 분석할 수 있었고, 효과적으로 차단 할수 있다는 결과를 도출 하였다. 앞으로 네트워크 시스템과 정보보호시스템과의 연동을 통한 다양한 분석이 가능한 예경보시스템을 개발하여 구성한다면 더욱 발전된 보안체계를 확립할수 있을 것이다.

지금의 시도는 위협에 대한 대처능력을 향상시키기 위한 포괄적 사이버위협 조기예경보위협시스템을 설계 가능성을 타진하는 것으로서 대형 네트워크의 사이버위협 대처능력 강화를 통해 대규모 피해 유발을 억제하고, 보안관리기관의 독자적인 정보보호시스템 운영으로 보안사고 발생에 신속, 능동적으로 대응할 수 있는 기능을 부여하고자 하는 노력이다.

참 고 문 헌

[1] 이상호, 국가위기관리차원에서의 사이버안보 확보방안 및 위기관리향상 프로그램 연구, 5, p. 45, 2004.

[2] 이동휘, 이강택, 김귀남, "허니넷을 이용한 악성트래픽 차단연"구, 정보보호학회추계논문지, 제1권, 제2호, pp. 97-101, 2004. 11.

[3] Nicolas Vanderavero, Xavier Brouckaert, Olivier Bonaventure, Baudouin Le Charlier, "The HoneyTank : a scalable approach to collect malicious Internet traffic", IEEE2004 RTSS04, Session 1, 2004. 12.

[4] 서동일, 최양서, 이상호, "실시간 침입자 행동 양식 파악 시스템의 설계 및 구현", 한국정보처리학회 2003년 춘계학술대회, Vol. 10, No. 01 pp. 1941-1944, 2003. 5.

[5] http://www.Honeynet.org, "Honeynet Project Overview", 2005. 4.

[6] 김영미, 네트워크보안의 현주소, ZDNET, 2004. 2

[7] 문호건, 최진기, 강유, 이명수, "취약점과 위협의 상관성 분석을 통한 네트워크 위험 조기경보 시스템 설계", 정보보호학회지, pp. 23-32, 2005. 2.

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