네트워크 보안상태 감시를 통한 침입탐지

황혜선*°, 이상호*, 임채호**

*°한국원자력연구소, *충북대학교 전자계산학과, **한국과학기술원 전자계산학과

Intrusion Detection through Monitoring of Network Security Status

Hyeseon Hwang*°Sangho Lee*, , Chaeho Lim**

*°Information & Network Management Division, KAERI, *Dept of Computer Science, Chungbuk Univ, **Dept of Computer Science, KAIST

요 약

Code Red, Nimda 등 최근 인터넷웜(Internet Worm)에 의한 침입은 방화벽시스템, 침입탐지시스템 등 보안제품이 존재하는 네트워크에서도 적절한 대책이 되지 않은 경향을 보이고 있다. 침입차단시스템을 통과할 수 있는 신종 취약점을 이용한 침입에는 오용방지방법(Misuse Detection)에 의한 침입탐지시스템이 침입패턴을 업데이트하기 전에 이미 네트워크에 피해를 입힐 가능성이 크게 증가하는 것이다. 향후에도 크게 증가할 것으로 보이는 인터넷웜 공격 등에는 침입차단시스템, 침입탐지시스템 등 보안제품의 로그기록 상황과 네트워크의 보안상태를 지속적으로 감시함으로서 조기에 침입을 탐지할 수 있다. 본 논문에서는 신종 웜 공격에 의한 침입이 발생되었을 때 IDS가 탐지하지 못하는 상황에서도 침입의 흔적을 조기에 발견할 수 있는 네트워크 보안 상태변수확인방법(Network Security Parameter Matching Method)을 제안하고자 한다.

I. 서론

인터넷 침입을 제대로 탐지하고 대응하려면 여러 정보보호 기술뿐 만 아니라 네트워크나 시스템의 각종 상황을 함께 파악하여야 제대로 최근 신종 공격을 확인할 수 있다. 대표적인 정보보호 기술제품으로는 침입차단시스템(Firewall), 침입탐지시스템(IDS), 접근제어시스템(Access Control), 취약점분석시스템(Scanner) 등을 고려할 수 있으나 최근 나타난 Code Red, Nimda 등의 인터넷 웜에 무기력한 대응을 보인 바 있다. 침입차단시스템은 80 포트를 공격하는 신종 취약점을 탑재한 웜 공격을 막지 못하였으며, 국내 소개되는 침입차단시스템은 대부분 오용탐지방법에 기반 하여 신종기법을 탐지하는 규칙이 업그레이드될 때까지 웜공격을 탐지하지 못하였다. 즉 침입을 막고 탐지 대응하는 기존의 보안기술은 신종기법에는 무용지물이 되어 초기대응이 신속하여야만 피해를 최소화할 수 있는 웜 공격에는 무력함을 알 수 있었다.

하지만 웜 공격의 특징이 네트워크에 많은 트래픽을 유발하여 누구나 네트워크의 장애로 인하여 신종 침입이 나타났음을 알 수 있었다. 네트워크의 정상적인 상태와 그렇지 않은 상태를 잘 감시하면 Firewall이나 IDS가 인지할 수 없는 침입을 조기에 탐지가 가능하다는 것이다.

그러므로 현재 보급된 침해사고 방지 대응용 정보보호제품 뿐만 아니라 네트워크의 상태를 감시할수 있는 네트워크 관리기술 등을 통합한 새로운 침입탐지기법 등이 요구된다.

본 논문에서는 인터넷 웜 등 최근 인터넷 공격기법의 발전 경향과 침입탐지시스템 관련 기술 등 관련 기술 현황을 살펴보고, IDS의 도움 없이 Code Red Worm 공격을 탐지 분석하여 대응책을 구현한 방법을 기술한다. 이러한 구현된 경험을

토대로 네트워크 보안상태변수를 파악하여 침입을 탐지하는 침입탐지의 새로운 방법론을 제시한다.

II. 관련 연구 및 기술동향

1. 침입기법의 발전

최근에 유포된 코드레드 웜은 버퍼 오버플로우를 이용한 DDoS(Distributed Denial Of Service) 공격과 백도어 설치로 인한 내부 데이터 변조, 삭제, 유출 및 스캔과정에서 높은 PPS(Packets Per Second)를 유발하여, 네트워크의 속도저하 및 마비까지 시키는 등 다양한 공격방법이 혼합되어 사용되고 있으며, 이런 악성프로그램이 해킹수법의 대다수를 차지하고 있다.

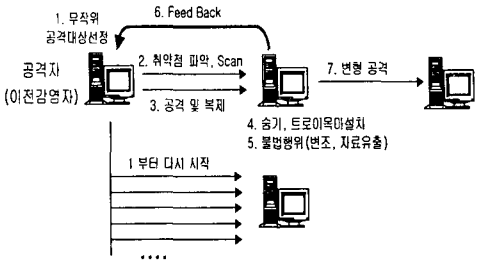
다음은 2001년 9월에 발생된 해킹수법에 대한 CERTCC-KR의 통계이다.

구분	건수	비고
사용자 도용	18	개인사용자계정 도용 등
S/W 보안 오류	4	IIS Unicode 관련 오류
버퍼오버플로우 취약점	20	named/bind 등의 취약점 이용
구성·설정 오류	1	사용자 권한 설정 오류
악성 프로그램	268	Code Red 웜, Code Blue 웜, Nimda 웜
프로토콜 취약점	0	-
서비스 거부 공격	4	Code Red 웜의 부작용
E-mail 관련 공격	6	스팸메일 관련 공격
취약점 정보수집	201	named/bind, ftpd, rpc 취약점 스캔
사회 공학	0	-

[표1] 해킹수법별 통계 (2001. 9)

인터넷 웜은 E-mail에 첨부되어 사용자의 도움으로 전파되는 웜[1]과 달리, 일단 인터넷 웜 프로그램이 시작되면 자동으로 취약성이 있는 시스템을 찾아서 공격하고, 공격이 성공하면 자기 자신을 피해시스템에 복제하고, 그리고 해당 피해시스템에서 또 다시 다른 시스템을 공격하는 메커니즘을 갖고 있다. 따라서 인터넷 웜의 전파속도는 취약한 목표시스템을 찾아내는 스캐닝 메커니즘에 따라 크게 달라진다.

공격 목표를 찾아내는 방법으로는 보통 무작위로 인터넷 전체를 검색하는 방법이 있으며, 종종 특정 공격목표를 공격하기 위해 특정 IP 주소 목록을 사용하는 경우가 있다. Code Red는 무작위로 공격대상을 정하는 방법을 사용했으며, 다음 버전인 Code Red II 는 IP 주소의 밀집성(Locality)을 이용한 공격이었다. 즉, Code Red II 는 공격에 성공하고 나면, 피해 시스템이 속한 같은 네트워크를 더 많이 공격하는 특징을 갖는다. 이는 공격 성공률을 증가시키며, 따라서 확산 속도도 더 빨라지게 된다.[3]



[그림1] Worm 공격 동작개념

2. 네트워크기반 IDS의 현황과 한계

최근 네트워크 기반의 IDS와 관련된 문제점들이 대두되고 있다. 네트워크 고속화로 인한 실시간 분석의 한계, 스위칭 기술로 인한 네트워크 기반 IDS의 탐지영역 제한, 유니 코드 결함 및 VPN 등의 암호화로 인한 침입분석의 어려움 등이 문제점으로 지적되고 있다.[5]

또한, 국내 대부분을 차지하고 있는 IDS는 오용탐지 기반이 대부분이므로 신종 침입수법에는 취약할 수밖에 없는 문제점을 갖고 있다. 오용탐지(Misuse Detection)는 일단 침입이 발견되고 침입패턴이 IDS에 적용된 후에야 해당침입을 탐지할 수 있기 때문에 실제 침입이 발생된 초기에 문제를 자동 탐지하는 것은 불가능하기 때문이다.

III. Code Red Worm 탐지 및 분석

1. 개요

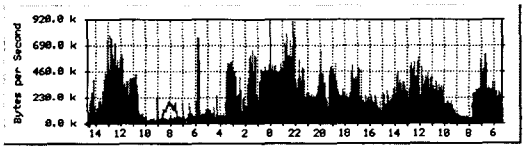
Code Red 웜에 의한 공격을 받고 있을 때 가장 먼저 네트워크에서 접속지연이 발생했으며, 그것이 침입인지, 바이러스인지, 다른 장애상황인지를 판단하기는 쉽지 않았다. 가장 먼저 NMS (Network Monitoring System)와 방화벽시스템 로그로 문제의 시스템을 찾을 수 있었고, 그 시스템의 로그에서 Code Red 웜으로부터 DDoS공격을

1) 기술적으로 정의하면 이는 트로이목마공격에 속한다고 볼 수 있으며, 바이러스 웜과는 매우 성격이 다른 것으로 간주하여야 한다.

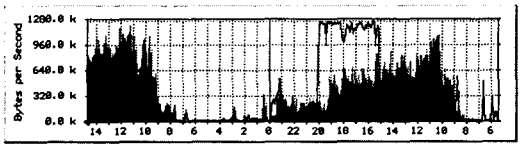
받고 있음을 확인했다. IIS 서버가 아니라서 감염은 되지 않았지만, 80 port를 대상으로 시도되는 DDoS 공격으로 인해 네트워크를 정상적으로 사용할 수 없었으며, 결국 라우터에서 필터링 기능과 액세스 리스트기능을 이용해서 공격을 막을 수 있었다.

2. 트래픽 분석을 통한 Code Red 징후 발견

Incoming 트래픽이 평소보다 급증된 현상을 보고 이상 징후를 파악할 수 있었다. 다음 그림에서 실선으로 나타난 그래프가 Incoming 트래픽을 나타내며, [그림2] 의 실선 그래프는 정상상태를, [그림3]의 실선 그래프는 Code Red 웜 공격으로 인한 Incoming 트래픽의 증가를 보여주고 있다.



[그림2] 네트워크 현황(정상상태)



[그림3] 네트워크 현황 (이상상태)

3. 방화벽을 통한 Code Red 분석

방화벽에서는 80 포트를 이용하는 공격이 1분당 7천-8천 개씩 계속되고 있었고, 트래픽을 기록으로 남겨 로그를 확인하여 해당 시스템의 IP 주소가 확인되었다. 공격 대상 IP 주소를 보호하기 위하여 방화벽 로그의 화면을 직접 캡쳐하지 않았음을 밝혀둔다.

19x.1xx.1x.117	211.245.34.250	tcp	80	3287
19x.1xx.1x.117	211.36.189.100	tcp	80	1764
19x.1xx.1x.117	211.176.255.216	tcp	80	2357

[표2] 방화벽 로그

4. 라우터, 방화벽에서의 대책 구현

필터링 기법을 이용하여 Code Red 공격을 막는 방법은 라우터와 방화벽시스템 모두에서 구현가능하나, 많은 양의 공격이 시도되고 있었으므로 라우터에서 Class-map을 이용한 필터링 기법으로 구현하였다.[4] 다음은 필터링 기법 구현 내용 중 일부이다.

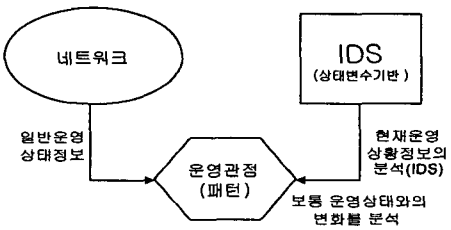
```
#class-map match-any http-hacks
(cmap)#match protocol http url "*default.ida*"
(cmap)#match protocol http url "*cmd.exe*"
(cmap)#match protocol http url "*root.exe*"
```

5. 보안상태변수파악 침입탐지방법론

1) 침입탐지 방법 제안

이상으로 지금까지 오용탐지기법에 기반한 IDS로 탐지할 수 없었던 Code Red를 NMS, 방화벽 등 네트워크 트래픽의 비정상적인 증가상태를 분석하여 탐지하고 대응한 기술적 방법을 소개하였다.

그렇다면 IDS나 방화벽은 신종 침투기법에 기인한 침입을 사전에 대응할 수 없음을 알 수 있었는데, 이러한 오용탐지가 아닌 네트워크 등에서의 비정상적인 패턴을 기반으로 네트워크를 감시하는 새로운 침입탐지 기법이 요구된다. [그림4]는 이러한 네트워크보안상태변수패턴매칭 방법론의 모델을 보여주고 있다.[1]



[그림 4] 운영상태변수기반 IDS 모델

이번 Code Red 경우에는 네트워크상태변수로서는 네트워크의 비정상 트래픽 증가가 주요한 변수로서 침입의 징후를 탐지하는데 매우 중요한 역할을 하였다. 이러한 변수는 DDoS공격 등 네트워크 트래픽을 증가시키는 방식의 경우 신속히 침입을 탐지하고 분석하는데, 도움이 될 것이다.

이러한 방법을 이용하여 단순히 IDS, 방화벽만으로 이루어진 기관의 네트워크의 침입대응을 바이러스 공격에 대한 백신 프로그램 갱신과 같은

모델로써 고려할 수 있다. 백신업체 대신 IDS 업체로 교체하여 다음 모델을 제안하고자 한다.

(1) 신종해킹기법 침입을 기존의 IDS는 탐지불가

(2) NMS 트래픽분석 등으로 신종해킹침입 징후 파악

(3) 방화벽로그 분석을 통하여 공격자, 피해자 서버를 확인한 후 공격프로그램 등 공격방식 파악

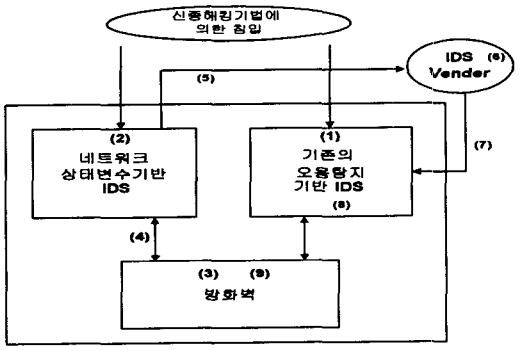
(4) 침입패턴 등을 상태변수에 첨가

(5) IDS 업체에 공격패턴 등 보고

(6) IDS 업체 오용탐지 패턴분석 Update

(7),(8) IDS에 패턴 Upgrade

(9) 방화벽에 패턴 접근제어 규칙 적용



[그림5] 백신Update방식을 응용한
신종해킹침투대응체계

2) 평가

보안상태변수 파악 침입탐지방법은 오용 탐지 기반의 IDS에서 탐지하지 못하는 신종침투기법에 대한 사전 탐지와 신속한 대응을 가능하게 한다는 점에서 기존의 IDS의 한계를 보완해 주는 적절한 방법으로 평가할 수 있겠다.

Ⅳ. 결론

본 연구를 통하여 신종 해킹기법에 의한 공격에는 기존의 오용탐지 기반의 네트워크 IDS는 침입을 탐지하는 것이 불가능하다는 것을 밝혀내고자 하였다. 결국 최근 발생한 대표적이 인터넷 웜인 Code Red를 대상으로 주어진 네트워크와 IDS가 공존하는 상태에서 검증하고자 하였다.

예상대로 IDS는 침입을 탐지하지 못하였고 NMS에서 네트워크 트래픽의 비정상적인 증가 상태를 파악하여 새로운 공격 징후를 발견하였으며, 방화벽에서의 기록을 바탕으로 어떤 시스템이 공격하는지 목표 시스템은 무엇인지, 그리고 피해를 당한 시스템에서 Code Red를 발견하고 공격패턴을 분석해 낼 수 있었다.

이를 토대로 방화벽과 라우터 등에서 더 이상 침입을 막을 수 있는 대응체계를 갖출 수 있었으며, 이러한 과정을 통하여 현재 IDS 에 의한 침입탐지 및 대응체계의 한계를 알수 있었다.

방화벽과 IDS는 침입대응체계를 갖추는데 매우 중요한 요소를 차지하지만 그 한계를 드러낸 상황이므로 네트워크 운영 상태변수의 확인방법에 기초한 IDS 모델을 함께 갖추어야만 바람직한 대응체계 모델을 확보한다는 사실을 깨닫고 새로운 IDS 인프라체계를 제시하였다.

이 연구의 성과로서는 Code Red를 대상으로 IDS의 새로운 방식을 제안한 것이며, 하지만 향후 보다 많고 상세한 네트워크 및 시스템의 정상적인 운영 변수를 발굴하여 신종해킹기법에 의한 공격을 보다 정확하게 탐지하고 분석할 수 있는 방법론의 개선이 요구된다.

참고문헌

[1] Edward Amoroso, Intrusion Detection, Intrusion.net Books, 1999

[2] Radware, "SynApps Architecture", http://www.radware.com

[3] Eeye digital Security, "CodeRedII Worm Analysis", http://www.eeye.com/

[4] CISCO Systems Inc, "Using Network-Based Application Recognition and Access Control Lists for Blocking", http://www.cisco.com/

[5] National Security Telecommunications Advisory, "Intrusion Detection Subgroup Report", http://www.ncs.gov/