신뢰 호스트 상호 협력을 통한 IP 스푸핑 공격의 효율적 탐지 및 방어 모델 설계

이해동* · 하현태** · 백현철** · 김창근*** · 김상복****

Efficient Detction and Defence Model against IP Spoofing Attack through Cooperation of Trusted Hosts

Hae-dong Lee* · Hyeon-tae Ha** · Hyun-chul Baek** · Chang-gun Kim*** · Sang-bok Kim****

요 약

오늘날 기업에서는 업무의 신속성과 내부의 중요 정보 자산의 보호를 위하여 많은 투자를 하고 있다. 하지만 내부 기업 망 전체를 모두 같은 수준의 방어 시스템으로 구축하기에는 많은 예산과 인력을 투입해야 하는 문제가 있다. 본 논문은 분산 관리되는 기업 망에서 공격자가 다른 신뢰 호스트를 이용하여 목표로 하는 시스템을 공격할 때 신뢰 호스트 상호간 정보 교환을 통하여 IP 스푸핑 공격에 대하여 효율적이면서 신속한 대응이 가능하도록 방어 모델을 설계 하였다.

ABSTRACT

Today, many enterprises have invested heavily for the part of information security in order to protect the internal critical information assets and the business agility. However, there is a big problem that big budget and too many manpower are needed to set the internal corporate network up to the same high level of defense for all of part. On the distributed enterprise networks in this paper, a defense model for effective and rapid response on the IP spoofing attack was designed to protect the enterprise network through the exchange of information between the trust hosts when an attacker attacked any target system using other trusted host.

키워드

트레이스라우트, IP 스푸핑, 신뢰 호스트, 네트워크 트래픽

Key word

Traceroute, IP Spoofing, Trusted Hosts, Network Traffic

* 정회원 : 경상대학교 컴퓨터과학과
** 정회원 : 경상대학교 컴퓨터과학과
*** 정회원 : 경남과학기술대학교 컴퓨터융합공학과
**** 정회원 : 경상대학교 컴퓨터과학과 교수 (교신저자, sbkim@gnu.ac.kr)

접수일자 : 2012. 06. 22
심사완료일자 : 2012. 08. 07

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.12.2649

Ⅰ. 서 론

일반적인 기업내 네트워크는 안정성과 보안성을 위하여 다양한 보안 장비를 운영하고 있다. 아울러 원격지 사용자간에는 상호 신뢰 가능한 네트워크 망 구성과 외부 공격에 대비한 방화벽, 침입탐지 시스템, 침입방지 시스템[1] 등을 단독 또는 복합적으로 운영하고 있다. 하지만 이러한 보안 시스템의 구축은 기업의 모든 정보가 집중관리 되는 곳과 일반적으로 자료를 업로드 하는 곳과의 구축정도에는 차이가 있다. 하지만 보안망 구축 정도의 차이는 IP 스푸핑[2] 공격 발생 시 공격자의 집중적인 표적이 될 수 있다. 일반적인 네트워크 보안 장비는 원격지 접속에 대한 보안 정책을 인가된 IP 주소의 인증 여부를 가지고 접근 여부를 결정한다. 특히 공격자는 보안 시스템이 집중되어 있는 네트워크 망에 대하여 직접 공격이 어려울 경우 해당 시스템에서 인증하고 있는 다른 신뢰 호스트를 이용하여 목표 시스템으로 접근하게 된다. 그러므로 본 논문에서는 이의 탐지를 위하여 각각 분산되어 있는 신뢰 호스트 상호간 트레이스라우트[3] 정보와 정상적인 연결 상태에서 측정 가능한 트래픽 정보를 수집하여, IP 스푸핑 공격에 대하여 효율적 대응이 가능한 모델을 설계 하였다. 본 논문의 구성은 Ⅱ장에서는 기존 IP 스푸핑 공격, 트레이스라우트 정보와 관련 정보 획득 과정, Ⅲ장에서는 시스템 구현을 위한 알고리즘과 제안 모델 설계, 그리고 Ⅳ장에서는 시뮬레이션 및 평가 그리고 그 결과 분석, 마지막 Ⅴ장에서는 결론 및 향후 과제에 대하여 정리하였다.

Ⅱ. 관련 연구

2.1. IP스푸핑 공격

IP 스푸핑은 공격자가 목표로 하는 시스템에 대하여 불법적인 접근을 하기 위하여 IP 패킷을 자신의 의도대로 조작한 후 패킷을 전송하여 목표 시스템을 속이고 접근하는 것을 의미 한다. 이 때 공격자는 목표 시스템이 신뢰하고 있는 신뢰 호스트의 접근 정보를 알아 낸 다음 해당 정보를 가지고 목표 시스템으로 접근을 시도한다. 패킷을 수신한 목표 시스템은 단지 패킷에 들어 있는 IP 주소만을 가지고 인증 여부를 판단하기 때문에 목표 시스템은 해당 패킷이 어디서 왔는지 명확하게 알 수가 없다. 즉 IP 자체의 보안 취약성을 악용하여 자신의 IP 주소를 목표 시스템에서 인증하고 있는 시스템의 주소를 이용하여 불법 접속을 시도하는 것이다[4]. 그림 1은 신뢰관계에 있는 두 시스템 사이에서 인증을 받지 않은 자가 자신의 IP 주소를 신뢰관계에 있는 사용자의 IP 주소로 바꾸어 목표 호스트를 속이고 접속을 시도하는 것을 나타내고 있다. 그 다음 rlogin, rsh 등을 이용하여 목표 호스트를 무력화 시킨다. 즉 공격자가 마치 목표 호스트가 신뢰하고 있는 접속자인 것 같이 위장하여 접속을 시도하는 침입 형태를 말한다.

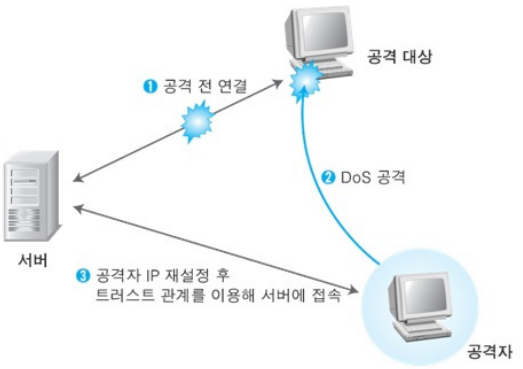


그림 1. IP 스푸핑의 예
Fig. 1 Example of IP spoofing

2.2. 트레이스라우트 정보

우리가 이용하고 있는 인터넷은 최종 목적지까지 직접적으로 연결되는 것이 아니라 중간에 여러 개의 경로를 거쳐 최종 목적지까지 연결된다. 트레이스라우트란 그림 2에서 보는 것과 같이 인터넷 경로를 배분하는 데 쓰이는 프로그램으로, 자신의 컴퓨터가 인터넷을 통해 최종 목적지를 찾아갈 때 각 구간마다 거치는 곳의 정보를 기록하는 유틸리티를 말한다. 트레이스라우트를 통해 IP 주소나 URL로 목적지를 입력하면 각 구간마다 지나는 게이트웨이 컴퓨터의 이름이나 주소, 걸리는 시간 등을 표시하기 때문에 인터넷 경로상의 정보를 획득할 수가 있다. 본 논문에서는 원격지의 정상적인 접속 트레이스라우트의 경로정보를 데이터베이스화 한 다음, 해당 정보를 이용하여 원격 접속을 시도하는 사용자들의 검증을 한다.

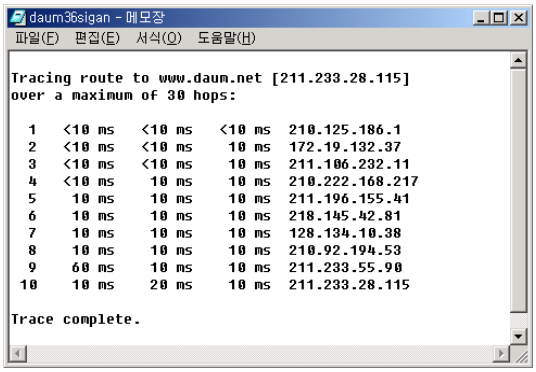


그림 2. 트레이스라우트 정보
Fig. 2 Traceroute information

2.3. 정상적인 트래픽 상태의 정보 정보획득

공격자는 IP 스푸핑 공격을 시도할 때 목표 시스템에서 신뢰하고 공격자 자신이 스푸핑에 이용할 신뢰 호스트를 무력화시키기 위해 DoS 공격 등 트래픽을 폭주시키는 사전 공격을 한다[5]. 그 다음 목표 시스템에서 인증을 하는 시스템의 IP 정보를 이용하여 목표 시스템으로 접근하게 된다. 본 논문에서는 일정기간 동안 원격지의 신뢰 호스트 간 접속자들의 접속 행위 중 트래픽의 변화를 분석하여 인증 시스템 각각의 상호 인증[6][7]을 위한 데이터베이스의 트래픽 정보로 활용하였다. 그 다음 트레이스라우트 정보와 결합하여 신뢰 호스트에 대한 트래픽 유발 공격의 방어와 차후 유사한 공격에 대비할 수 있도록 하였다.

Ⅲ. 사전 탐지 모델 설계

3.1. 제안모델 설계

본 논문에서 제안하는 트레이스라우트 정보를 이용해 각 신뢰 호스트에서 불법적인 공격을 탐지 하는 과정은 다음과 같다.

Step 1 : 침입자는 타겟 호스트가 신뢰하고 있는 해당 신뢰 호스트의 IP 주소 정보를 획득한다.

Step 2 : 해당 신뢰 호스트의 정보를 획득한 침입자는 DoS, DDoS 공격을 시도하여 자신이 위장할 신뢰 호스트를 다운시킨다.

Step 3 : 침입자는 자신의 IP주소를 해당 신뢰 호스트의 IP로 변경 시킨 후 IP 스푸핑 공격을 시도한다.

Step 4 : 타겟 호스트는 접속을 시도한 IP주소가 OUT_IN (외부에서 내부로 접근)값을 가지므로 트레이스라우트를 실시하여 접속자의 정상 유.무를 판단한다.

Srep 5 : 타겟 호스트의 방어 시스템에 존재하지 않는 경로로 판정되면 확인을 위한 원-타임 패스워드 전송한다.

Step 6 : 원-타임 패스워드 불일치 시 접속을 차단한다.

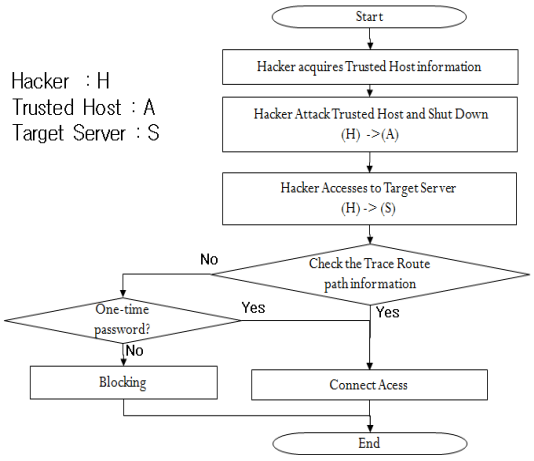


그림 3. 트레이스라우트 정보를 이용한 차단 과정
Fig. 3 Blocking process using the traceroute

상호 신뢰하는 호스트 간 트래픽 수집은 단위시간당 리시버에 성공적으로 도착한 초당 비트수인 처리량(throughput)을 수집하였다. 처리량의 수집을 위해 지수적(exponential)인 트래픽을 생성하였으며 그 지속시간은 600초로 설정하였다.

그리고 생성한 트래픽의 전송을 위하여 사용자 정의의 태스크 형태를 그림 4와 같이 설정하였다. 그림 6에서 보는 바와 같이 전송을 위한 프로토콜은 TCP를 사용하였다. 이는 스푸핑의 다양한 형태 중 신뢰 관계의 악용을 유발하는 IP 스푸핑의 특성을 활용하여 트래픽을 생성한 것이다.

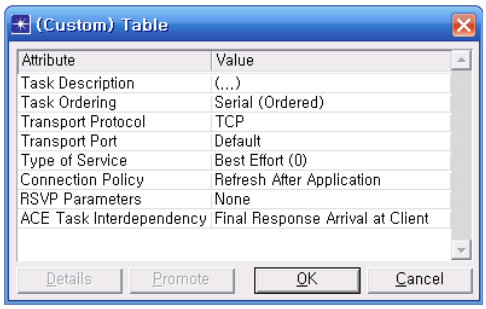


그림 4. 발생 트래픽 형태
Fig. 4 The traffic of the form

공격 대상 서버의 트래픽은 요구(request)와 응답(response)에 대한 병행처리가 가능하게 설정하였다.

3.2. 상호 신뢰정보를 이용한 공격자 탐지과정

본 논문에서 구축하고자 하는 불법 사용자들의 신뢰 호스트에 대한 접근 탐지과정은 다음과 같다. 불법 사용자는 목표 시스템의 접근 정보인 로그인 아이디와 패스워드, 그리고 외부에서 내부망으로 접근 가능한 신뢰 호스트의 IP를 알아낸 다음 원격 접속이 가능한 TELNET이나 FTP 포트를 통하여목표 시스템으로 접근을 시도한다[9]. 본 논문에서는 신뢰 호스트 간 생성되어 있는 인증 데이터베이스를 이용하여 원격지 접속자의 접속 여부를 결정한다. 상호간 인증을 하고 있는 각 신뢰 호스트들은 그림 5와 같은 상호 인증 데이터베이스 정보를 공유하고 있다.

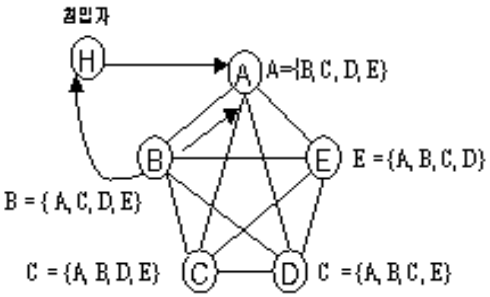


그림 5. 신뢰 호스트 상호간 구성 정보
Fig. 5 Trace information composition between trusted host

만일 정상적인 사용자가 각 신뢰 호스트에 등록되어 있지 않은 전혀 새로운 지역에서 접속을 시도할 경우에는 이미 구축 해 놓은 사용자 로그인 정보와 트레이스라우트 정보를 비교하여 검증을 한다.

Ⅳ. 시뮬레이션 및 평가

4.1. 실험

본 논문에서 제안하고 있는 방어 시스템과 관련하여 사용된 응용 소프트웨어는 VisualStudio 6.0, OPNET이며, 구현언어는 Visual C++을 사용하였다. 제안 시스템에 대한 시뮬레이션 환경 중 장비의 운영체제는 WindowsXP이고, 시스템 사양은 8GB 메모리를 채택한 Xeon E5506 2.13 Ghz Dual System으로 구성하였다. 그림 6은 본 논문에서 제안하고 있는 방어 시스템의 실험을 위한 OPNET의 구성도이다. 구성에 사용된 요소는 다음과 같다. 먼저 실제의 네트워크 환경에서 경로를 지정해 주는 라우터와 데이터베이스를 접근하는 웹서버, 해당 데이터베이스가 탑재되어 운영되는 백-엔드 데이터베이스 서버가 있다. 본 논문에서 웹서버와 백-엔드 데이터베이스 서버의 구성은 일반적인 웹 환경으로 별도 구성을 하였다.

그리고 각 신뢰 호스트들은 엔터프라이즈 네트워크 내부의 신뢰그룹으로 정의 하였다. 해당 구성에 대한 설정은 신뢰 호스트간 광대역 접속이 가능하도록 하였다. 아울러 인가된 사용자에 한하여 웹서버에 대한 접근을 허용하고, 접근이 허가되지 않은 사용자는 기본적으로 웹 서버에 대하여 접근이 불가능 하도록 설정하였다. 그러므로 공격자는 백-엔드 데이터베이스 서버가 신뢰하고 있는 웹서버로 접근을 하기 위해서는 신뢰 호스트들이 상호 인증 정보로 이용하는 IP 주소를 획득한 다음 공격을 시도한다. 그리고 웹 서버에 대한 DoS, DDoS 공격을 시도하여 웹 서버를 무력화 시킨다. DoS, DDoS 공격으로 웹 서버가 다운되면 공격자는 백-엔드 데이터베이스 서버에서 신뢰하는 웹 서버의 IP 주소를 이용하여 IP 스푸핑 공격을 시도하는 것으로 공격 시나리오를 설정하였다.

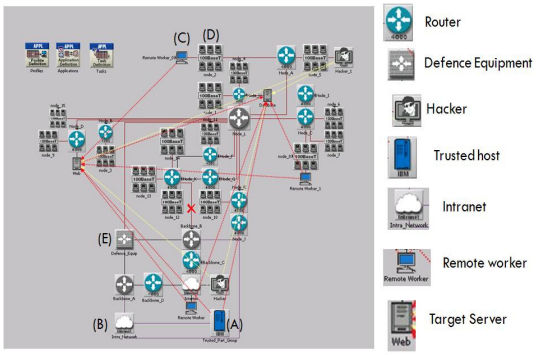


그림 6. 시스템 구성도
Fig. 6 System composition map

공격 상황 시뮬레이션 결과 확인을 위해 신뢰 호스트(A)와 인트라네트워크(B), 리모트워크(C)와 노드(D), 방어장비(E), 이렇게 3개의 구역에서 처리량을 추출하였으며 그 결과는 아래의 그림 7과 같다.

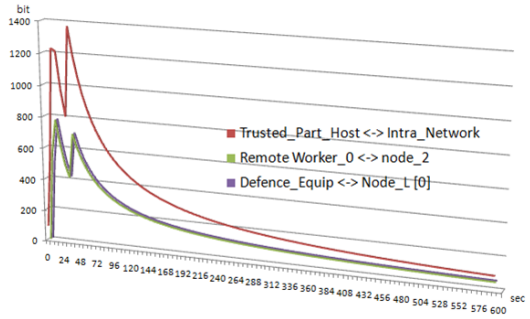


그림 7. throughput 결과
Fig. 7 The results of throughput

그림 7에서 보이는 범례의 첫 번째 그래프가 (A)와 (B)를 통과하는 throughput이고, 두 번째 그래프가 (C)와 (D)를 통과하는 throughput이며 마지막 그래프가 (D)를 통과하는 throughput이다.

먼저 신뢰 호스트(A)에서 감지한 리퀘스트 처리량이 36초 동안은 증가되다가 이후로 감소하는 결과를 나타내는 것은 일반적으로 발생할 수 있는 비정상적인 트래픽에 대하여 바로 차단을 하게 되면, 서비스 가용성을 해칠 수 있기 때문에 36초 정도의 간격을 두었다. 만일 신뢰 호스트(A)에 리퀘스트 되는 데이터가 정상적인 경우의 트래픽인지 판단하는 과정을 거친 후 비정상 데이터라고 판단되면, 방어 장비에서 차단을 하기 때문에 그 처리량이 지속적으로 감소하는 과정을 볼 수 있다. 위 그림 7의 신뢰 호스트(A)와 인트라 네트워크(B)의 처리량 도표 중 0 ~ 90초 구간을 확대하면 그림 8과 같다.

time (sec)	Trusted_Part_Host <-> Intra_Network
0	96
6	565.3333
12	1235.556
18	1218.667
24	974.9333
30	812.4444
36	1379.048
42	1206.667
48	1072.593
54	965.3333
60	877.5758
66	804.4444
72	742.5641
78	689.5238
84	643.5556
90	603.3333

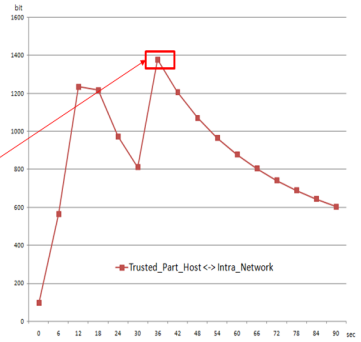


그림 8. 신뢰호스트(A)와 인트라네트워크(B)간의 처리량 결과
Fig. 8 Trusted host(A) and intra-network(B) between the thougthput Results

다음으로 그림 9는 리모트 워커(C)와 노드(D)사이에서 발생한 처리량 역시 비정상적인 트래픽이 발생 한 후 36초간 지속되다가 감소하는 과정을 보이고 있다.

time (sec)	Remote Worker_0 <-> node_2
0	0
6	557.3333
12	778.6667
18	623.3333
24	498.6667
30	415.5556
36	697.5238
42	610.3333
48	542.5185
54	488.2667
60	443.8788
66	406.8889
72	375.5897
78	348.7619
84	325.5111
90	305.1667

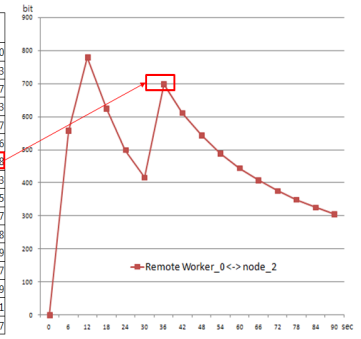
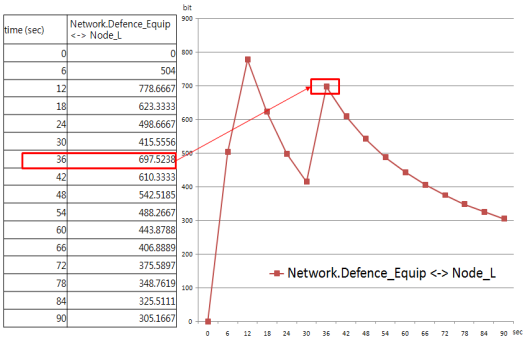


그림 9. 리모트워커(C)와 노드(D)사이의 throughput 결과
Fig. 9 Remote Worker(C) and node(D) between the throughput results

마지막으로 방어 장비에서 처리되고 있는 처리량도 그림10과 같은 형태로 나타나는 것을 알 수 있다.



time (sec)	Network.Defence_Equip <-> Node_L
0	0
6	504
12	778.6667
18	623.3333
24	498.6667
30	415.5556
36	697.5238
42	610.3333
48	542.5185
54	488.2667
60	443.8788
66	406.8889
72	375.5897
78	348.7619
84	325.5111
90	305.1667

그림 10. 방어장비(E)의 throughput 결과
Fig. 10 Defense equipment(E) in the throughput results

그림 11은 실제로 DDoS 공격으로 이상 트래픽이 발생하면 자신이 이미 구축해 놓은 트래픽 양에 대한 정보를 이용하여 이상 트래픽을 유발시킨 IP 주소를 가진 호스트를 차단하는 과정을 보여주고 있다.

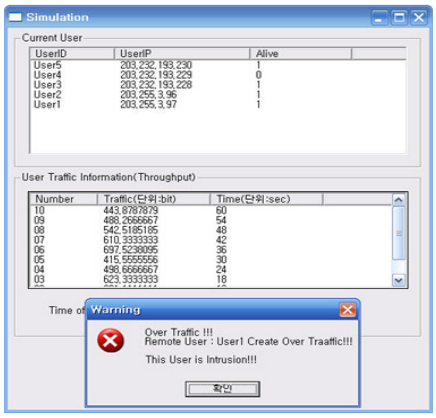


그림 11. DDoS 공격에 대한 차단 결과
Fig. 11 DDoS attacks on block results

또한 트레이스라우트 정보를 이용하여 차단한 결과를 보여주고 있다. 접속을 요청한 IP 정보를 이용하여 획득한 Tracing_temp 정보와 일상적인 상황 하에서 획득해 각 신뢰 호스트의 방어 시스템에 구축되어 있는 트레이스라우트 정보를 비교한 후 해당 IP 정보가 상이하므로 바로 차단되는 것을 그림 12에서볼 수 있다.

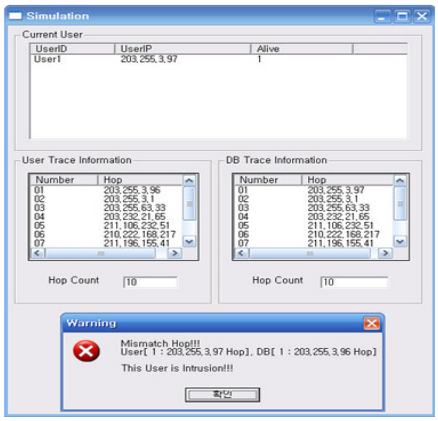


그림 12. 트레이스라우트 정보를 이용한 차단 결과
Fig. 12 Blocking result using the traceroute of information

V. 결론 및 향후 과제

본 논문에서 제안하는 IP 스푸핑 공격에 대한 효율적인 탐지 및 방어 모델은 먼저 신뢰 호스트간의 정상적인 트래픽 처리량 정보를 IP 스푸핑 공격을 시도하는 공격자의 행위를 탐지하기 위하여 정상적인 트래픽 상태의 처리량을 데이터베이스화 해 놓은 것이다. 만일 공격자가 목표 시스템에 대한 불법 접속을 시도하기 위하여 신뢰 호스트로 트래픽 유발 공격을 시도하면, 자신이 가지고 있는 해당 정보와 비교하여 공격자의 트레이스라우트 정보를 획득한다.

그 다음 해당 정보를 상호 신뢰하는 모든 호스트로 통보를 하기 때문에 1차 공격을 받지 않은 다른 신뢰 호스트들이 능동적으로 2차 공격에 대비 할 수 있다. 그러므로 1차 공격에 실패한 해커가 다른 신뢰 호스트를 공격 할 경우 해당 호스트는 즉각 차단이 가능하기 때문에 효율적인 방어가 가능하다. 또한 본 논문에서 제안하는 효율적인 탐지 개선 모델은 하드웨어적인 비용의 추가부담과 관리 인력의 추가 투입이 거의 없다고 할 수 있다. 향후 고려해야할 부분은 모바일 접속 상황에

서의 불법 접속 가능성에 대한 연구가 병행되어야 할 것이다.

참고문헌

[1] 하현태, 이해동, 백현철, 김상복, “엔터프라이즈 네트워크에서 DDoS 공격의 부하개선을 위한 큐잉 모델”, 한국해양정보통신학회논문지, 제15권 제1호, pp.107-114, 2011.

[2] 전준상, 정연서, 소우영, “패킷 스니핑과 IP 스푸핑을 이용한 TCP/UDP 패킷 생성기의 설계” 한국정보과학회 2005 가을 학술발표 문집(Ⅰ)제32권, 제2호, pp.649-651, 2005.

[3] 정종민, 이지율, 이구연, “역추적 에이전트를 이용한 역추적 시스템 설계 및 구현”. 강원대학교 산업기술연구소, Vol.22 No.B, pp.147-153, 2002.

[4] 이용호, 박희운, 이임영, “새로운 일회용 패스워드 방식 제안”. 한국정보처리학회 춘계학술발표 논문집, 4, 2001.

[5] Yun-Ji Ma, Hyun-Chul Baek, Chang-Geun Kim, Sang-Bok Kim, "Prevention of DDoS Attacks for Enterprise Network Based on Traceback and Network Traffic Analysis," International Journal of Maritime Information and Communication Sciences, v.7, no.2, pp.157-163, 2009.

[6] 김봉한, 이재광, 백승현, 오형근, 박응기, “침입 탐지 도구에서 능동 대응 정책 생성 방안”, 한국콘텐츠학회논문지, Vol.6 No.1, pp.151-159, 2006.

[7] 손형서, 김현성, 부기동, “암호화 기법을 적용한 침입 탐지 시스템의 보호 기법”. 정보보호학회 논문지, Vol.14 No.6, pp.3-13, 2004.

[8] 오재철, 김병철, “소규모 사설망 보호를 위한 방화벽에 관한 연구”, 順天大學校 論文集, 제19권, 제2호, pp.227-237, 2000.

[9] 이수진, 정병천, 김희열, 이윤호, 윤현수, 김도환, 이은영, 박응기 “연관성을 이용한 침입탐지 정보 분석 시스템의 설계 및 구현”. 정보과학회 논문지, Vol.31 No.5, pp.438-449, 2004.

저자소개

이해동(Hae-Dong Lee)

2009년 경상대학교 컴퓨터과학과 (공학석사)
2012년 현재 경상대학교 컴퓨터과학과 (박사수료)
2012년 현재 (주)이지시스 대표이사
※관심분야 : 네트워크, 네트워크보안

하현태(Hyeon-Tae Ha)

2008년 한국국제대학교 컴퓨터공학과 (공학사)
2011년 경상대학교 컴퓨터과학과 (공학석사)
2012년 현재 경상대학교 컴퓨터과학과(박사과정)
※관심분야 : 네트워크, 네트워크보안

백현철(Hyun-Chul Baek)

1998년 경상대학교컴퓨터과학과 (교육학석사)
2003년 경상대학교 컴퓨터과학과 (공학박사)
2007년 전국지방의료원 전산기술위원장
1988년~2011년 진주의료원 전산실장
2012년 현재:경상대학교 컴퓨터과학과 시간강사
※관심분야 : 네트워크, 네트워크보안, 암호화

김창근(Chang-geun Kim)

1999년 경남대학교 (공학박사)
2012년 현재 경남과학기술대학 융합기술공과대학장
2012년 현재 경남과학기술대학교 컴퓨터융합공학과 교수
※관심분야 : 데이터통신 및 이동통신, 홈네트워킹, 유비쿼터스 네트워킹

김상복(Sang-Bok Kim)

1989년 중앙대학교 전자공학과 (공학박사)
1984년~현재 경상대학교 컴퓨터과학과 교수
2000년~현재 경상대학교 컴퓨터정보통신연구소 연구원
2007년~2010년 경상대학교 교육정보전산원장
※관심분야 : 멀티미디어 통신, 컴퓨터네트워크, 컴퓨터구조