에이전트기반의 IP 역추적 시스템 설계 및 구현

채철주, 이성현, 김지현, 이재광

IP Traceback System Design and Implement based on Agent

Cheol-Joo Chae, Seoung-Hyeon Lee, Ji-Hyun Kim, Jae-kwang Lee

요 약

최근의 정보보호 환경에서는 자신의 관리 도메인 내로 침입하게 되는 공격을 어떻게 잘 탐지 할 것인가와 탐지된 공격을 어떻게 효율적으로 차단하여 자신의 도메인을 잘 보호할 것인가에 초점이 맞추어 있다. 따라서 탐지된 침입의 공격자에 대한 대응도 자신의 도메인 경계에서 해당 트래픽을 차단하는 수동적인 방법 이외에는 별다른 방법이 없는 상태이고, 이 경우 자신의 도메인에서 파악한 침입자 정보를 바탕으로 자신의 도메인 입구에서만 해당 트래픽을 차단함으로써 침입자는 자유로이 인터넷을 이용할 수 있을 뿐만 아니라 다른 공격 기술이나 공격 루트를 이용한 제2, 제3의 공격이 이루어 질 수 있다. 반면 인터넷을 이용한 경제 활동 및 그 액수가 점차 증가함에 따라 사이버 공격으로 입게 되는 피해는 점차 기업의 생존을 위협하는 수준에 도달하고 있다. 따라서 해킹에 능동적으로 대응할 수 있는 기술이 요구된다고 할 수 있으며, 능동적인 해킹 방어를 위한 가장 기본적인 기술로 해커의 실제 위치를 추적하는 역추적 기술을 활용할 수 있어야 한다. 그러나 현재까지 제안된 역추적 기술들은 인터넷이 보유한 다양성을 극복하지 못하여 현재의 인터넷 환경에 적용하는데 어려움이 따른다. 이에 본 논문에서는 해킹으로 판단되는 침입에 대하여 효율적으로 역추적 하기 위해서 iTrace 메시지를 이용한 역추적 시스템을 설계하고 구현한다.

Ⅰ. 서 론[1)]

컴퓨터 기술의 발달과 더불어 인터넷의 발전은 데이터 전송 속도의 과속화와 대용량의 데이터 전송 등의 기술을 증가시켜 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화시켜주는 긍정적인 효과를 가져온 반면, 인터넷의 확장으로 인하여 외부의 시스템 불법 침입, 중요 정보의 유출 및 서비스 거부 공격 등의 역기능들이 계속해서 증가되어 그 피해가 심각한 수준이다.

최근의 정보보호 환경에서는 자신의 관리 도메인 내로 침입하게 되는 공격을 어떻게 잘 탐지 할 것인가와 탐지된 공격을 어떻게 효율적으로 차단하여 자신의 도메인을 잘 보호할 것인가에 초점이 맞추어 있다. 따라서 탐지된 침입의 공격자에 대한 대응도 자신의 도메인 경계에서 해당 트래픽을 차단하는 수동적인 방법 이외에는 별다른 방법이 없는 상태이고, 이 경우 자신의 도메인에서 파악한 침입자 정보를 바탕으로 자신의 도메인 입구에서만 해당 트래픽을 차단함으로써 침입자는 자유로이 인터넷을 이용할 수 있을 뿐만 아니라 다른 공격 기술이나 공격 루트를 이용한 제2, 제3의 공격이 이루어 질 수 있다. 반면 인터넷을 이용한 경제 활동 및 그 액수가 점차 증가함에 따라 사이버 공격으로 입게되는 피해는 점차 기업의 생존을 위협하는 수준에 도달하고 있

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

다. 따라서 해킹에 능동적으로 대응할 수 있는 기술이 요구된다고 할 수 있으며, 능동적인 해킹 방어를 위한 가장 기본적인 기술로 해커의 실제 위치를 추적하는 역추적 기술을 활용할 수 있어야 한다. 그러나 현재까지 제안된 역추적 기술들은 인터넷이 보유한 다양성을 극복하지 못하여 현재의 인터넷 환경에 적용하는데 어려움이 따른다[1].

이에 본 논문에서는 해킹으로 판단되는 침입에 대하여 효율적으로 역추적 하기 위해서 iTrace 메시지를 이용한 역추적 시스템을 설계한다. 2장에서는 역추적 시스템을 동향을 분석하여 보고, 3장에서는 역추적 시스템을 설계하고 4장에서는 역추적 시스템에서의 패킷 모니터링에 대해서 살펴보고 5장에서는 결론을 맺고 향후 연구방향을 기술하였다.

II. 관련연구

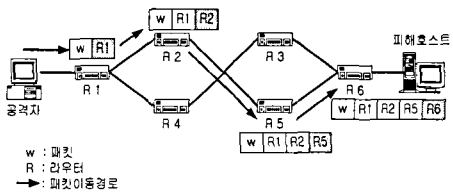
2.1 Packet Marking 기법

패킷 마킹 기법이란 네트워크를 순회하면서 지나간 라우터의 IP 주소를 패킷 속에 삽입하는 방식으로 마킹된 패킷을 받은 호스트는 라우터 주소 정보를 이용하여 지나온 경로를 구성할 수 있게 한 것이다.

패킷 마킹은 TCP/IP 프로토콜 중에서 IP 헤더의 Record Route option을 이용하여 IP 헤더의 옵션 필드에 라우터의 주소를 저장하거나 IP 헤더의 Identification 필드에 라우터 주소를 저장할 수 있는 것을 활용한 기법으로 Node Append 기법, Node Sampling 기법, Compressed Edge Fragment Sampling 기법 등이 있다.

2.2 Node Append 기법

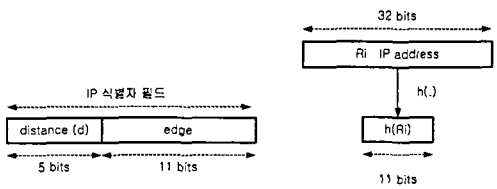
마킹 기법중 가장 간단한 Node Append 기법은 공격자의 패킷이 네트워크를 지나갈 때 노드의 주소를 공격자의 패킷에 추가해서 이 주소를 이용하여 공격자의 위치를 역추적 하는 기법이다. 피해 호스트에서는 받은 모든 패킷은 지나온 경로를 순차적으로 가지고 있기 때문에 역추적 경로를 구성하는데 시간이 짧다. 하지만 라우터들의 오버헤드와 경로의 전체 길이를 알 수 없기 때문에 패킷 공간 확보의 어려움이 있고 공격자가 거짓된 정보로 공간을 채울 수도 있다.



[그림 1] Node Append 기법

2.3 Advanced Marking Scheme I

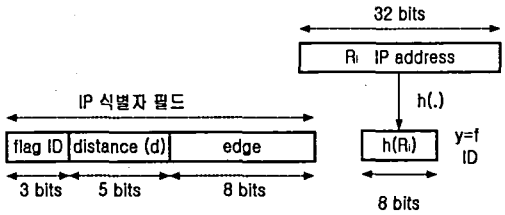
이 기법은 [그림 2]에서 나타나듯이 IP 식별자 필드 16비트를 마킹 필드로 사용하기 위해 피해 호스트로부터 라우터의 거리를 나타내는 5비트의 거리필드와 11비트의 edge 필드로 구분한다. 5비트의 거리필드는 32홉을 표시할 수 있으므로 인터넷 경로들을 충분히 나타낼 수 있다. 패킷의 IP 식별자 필드에 32비트의 라우터 주소를 hash 함수를 이용하여 11비트로 암호화한 후 마킹하게 된다. 그 후 각 라우터를 경유할 때마다 XOR 연산을 통해 라우터의 정보를 암호화하여 마킹하게 되고, 공격경로를 재설정하게 된다[2].



[그림 2] Advanced Marking Scheme I 인코딩 구조

2.4 Advanced Marking Scheme II

이 기법은 2개의 hash 함수를 사용하는 대신 독립적인 hash 함수 세트를 이용하는 것이다. Advanced Marking Scheme II 는 IP 헤더의 식별자 필드의 16비트를 마킹할 필드로 사용하는 것은 동일하지만 flag ID라는 필드를 추가하였다. 거리 필드는 32 홉을 표현할 수 있는 5비트를 그대로 사용하며 edge 필드는 flag ID 필드를 뺀 8비트가 사용된다. [그림 3]은 Advanced Marking Scheme II 인코딩 구조를 나타낸다[2].



[그림 3] Advanced Marking Scheme II 인코딩 구조

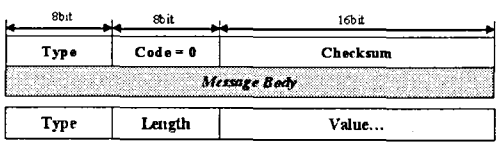
III. iTrace 메시지를 이용한 역추적 시스템 설계

3.1 iTrace 메시지를 이용한 역추적 기법

iTrace 메시지를 이용한 역추적 기법은 라우터에 거쳐 가는 패킷에 대해서 패킷의 일부가 포함된 ICMP 역추적 패킷을 생성하고 목적지 주소로 전송하고, 전송 받은 시스템은 해당 정보를 수집하여, 공격이 검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다.

3.2 iTrace 메시지(ICMP Traceback Message)

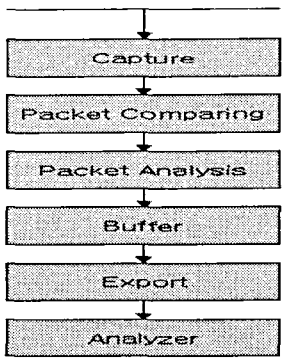
iTrace 메시지(ICMP Traceback Message)는 ICMP 패킷의 Message Body에 일련의 스트링으로 포함된다. ICMP Traceback Message를 위한 ICMP Type은 현재 정의되지 않았지만, IANA에서 조만간 정의 할 예정이다. Code 필드는 항상 '0' 으로 설정되며, Message Body는 하나의 이상의 TLV (Type-Length-Value) 엔트리로 구성된다. [그림 4]은 ICMP 역추적 메시지 형태를 보여주고 있다[3][4].



[그림 4] ICMP Traceback Message 형태

3.3 에이전트 시스템 설계

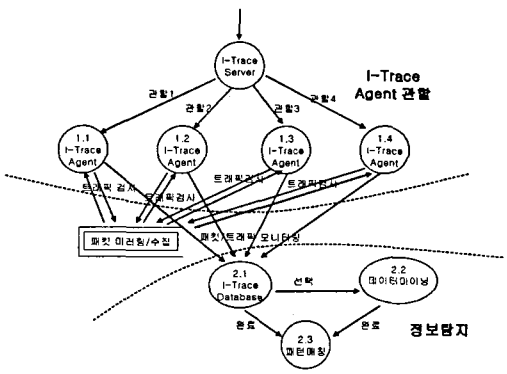
에이전트 시스템은 특정 IP에서 비정상 트래픽 현상이 발생하면 해당 IP를 감시하고, 발생시 문제 시스템을 손쉽게 찾아 해당 시스템의 정보와 수상한 Source IP를 서버에 신고하게 된다.



[그림 5] I-Trace 에이전트 트래픽 분석 흐름도

3.4 서버 시스템 설계

서버 시스템은 I-Trace 에이전트가 설치된 네트워크 전체를 아래 그림처럼 관할하고 통제할 수 있도록 구현되었다. 또한 I-Trace 서버의 메인 프로그램은 사용자에게 관할하는 네트워크의 현황을 실시간으로 모니터링 해주는 기능을 제공하도록 구현되었으며, 각 에이전트들은 자신이 가진 네트워크 관리 정보를 서버와 통신을 통해 교환하면서 유기적인 공격탐지 및 대응 프로세스를 처리하도록 개발 하였다.



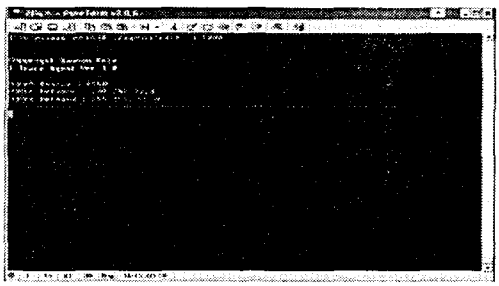
[그림 6] I-Trace System 구성 예시

IV. 패킷 감시 및 공격자 역추적

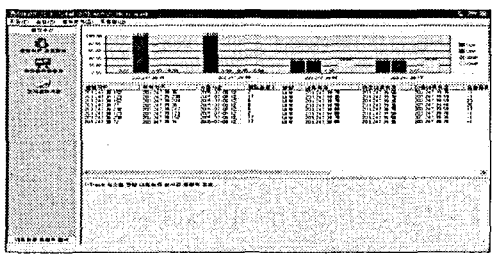
4.1 네트워크 패킷 감시

에이전트 시스템에서는 관리자가 설정한 네트워크 임계치에 따른 패킷 수집을 제공하며, 패킷 헤더 정보를 iTrace 메시지 생성 모듈에 전송하게 된다. [그림 7]은 에이전트 시스템에서 임계치를 설정한 모습을 보여주고 있다. 그리고 [그림 8]은

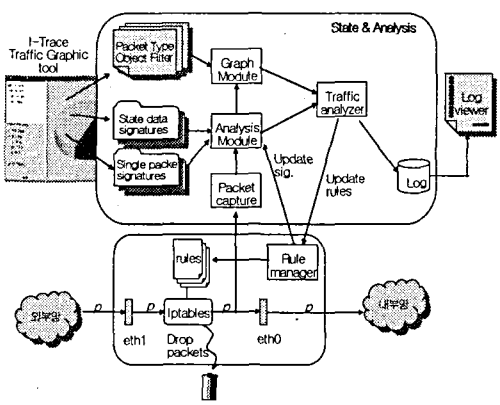
네트워크내의 패킷을 감시하는 모습을 보여주고 있다. [그림 9]은 다양한 원시 데이터의 분석 단계별 과정을 거쳐 최대한 효율적인 가공을 통해 얻어지는 과정을 보여주고 있다.



[그림 7] 임계치 설정 화면

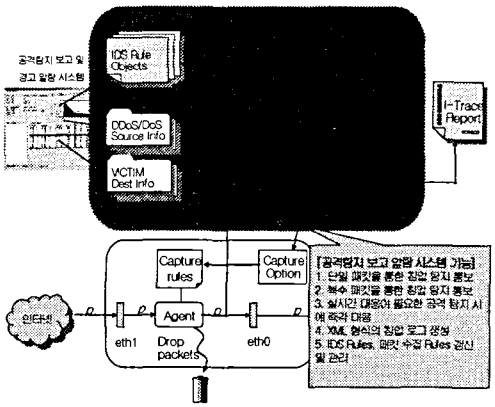


[그림 8] 네트워크 모니터링



[그림 9] 트래픽 통계 모듈 작업

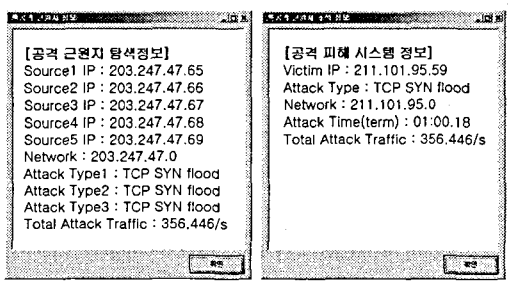
[그림 10]는 공격탐지 제어 이벤트에 대하여 실시간 통보가 가능한 알람 시스템을 나타내고 있다. 알람 시스템은 IDS 타입이나 보안정책 위반 등의 자세한 감시 및 관리도구로 쓰일 수 있다.



[그림 10] I-Trace DDoS/DoS 공격탐지 통보 및 경고 알람 시스템 Architecture

4.2 공격 경로 재구성

에이전트 시스템들은 서버로부터 통보된 공격 패킷정보를 기반으로 공격패킷으로 의심되는 패킷들을 검사해 해당 공격 유형과 일치하는 패킷을 찾아낸다. 이렇게 일치하는 추적정보들을 모아서 Victim IP를 기준으로 정렬하고, 라우터에서 라우팅 테이블이 갱신되는 시간 간격을 갖도록 앞서 정렬된 추적정보를 시간에 따라서 그룹화를 한다. 그런 다음 각 그룹에 속하는 데이터별로 라우터(에이전트) 주소, 패킷이 유입된 인터페이스 등의 정보를 갖는 역추적 노드를 생성한다. 이런 과정을 각 네트워크에서 반복하여 최종적인 공격 경로의 재구성이 이루어지게 된다.



[그림 11]Attacker와 Victim 정보화면

V. 결론 및 향후 연구 방향

인터넷 사용자의 급속한 증가로 인한 복잡한 TCP 반응과 연관되어 네트워크 서비스에 많은 패킷 손실을 야기하게 되었다. 이러한 문제를 해결하기 위하여 대학 연구소와 기업체에서는 침입

대응 시스템을 개발하게 되었고, 공격자의 근원지를 추적하는 역추적 시스템이 등장하게 되었다. 따라서 본 논문에서는 이러한 침입에 대한 대응을 위해 ICMP 기반의 역추적 시스템을 분석 및 설계하였다. 향후 연구로는 세밀한 분석을 통하여 모듈을 설계하고, 이 설계를 바탕으로 역추적 Agent와 역추적 Manager를 구현하고자 한다. ICMP 역추적 메시지는 현재 IETF internet Area의 itrace Working Group에서 Internet draft로 제출된 상태이다. ICMP 역추적 기법은 라우터에 거쳐가는 패킷에 대해서 패킷의 일부가 포함된 ICMP 역추적 패킷을 생성하고 목적지 주소로 전송하고, 전송 받은 시스템은 해당 정보를 수집하여, 공격이 검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다. 더 나아가 이를 능동 네트워크 기반으로 발전시켜 새로운 역추적 시스템을 구현하고자 한다.

참고문헌

[1] Chun He, Formal Specifications of Traceback Marking Protocols , June 14, 2002.

[2] 강호호외 3명, "IP 역추적 기술 동향", 주간기술동향, 97-39 한국전자통신연구원

[3] Steve Bellovin외 2명, "ICMP Traceback Messages", Internet Draft, IETF, Feb. 2003.

[4] Allison Mankin외 4명, "On Design and Evaluation of Intention-Driven ICMP Traceback"

[5] 이형우, "DDoS 해킹 공격 근원지 역추적 기술" 정보보호학회지, 2003.10

[6] S. Savage, D. Wetherall, A. karlin, and T. Anderson, "Network Support for IP Traceback", IEEE/ACM transactions on networking, vol. 9, No. 3, June 2001.

[7] R. Stone, CenterTrack: An IP overlay network for tracing DoS floods , in Proc, 2000 USENIX Security Symp., July 2000, pp. 199-212.

[8] D. Song and A. Perrig, Advanced and authenticated marking schemes for IP Traceback , in Proc. IEEE INFOCOM, vol. 2, April 2001, pp. 878-886.

[9] 이만영, 손승원, 조현숙, 정태명, 채기준 "차세대 네트워크 보안 기술" 생능출판사, pp.415-430, 2002.11.2