파밍 공격 대응을 위한 역추적 시스템 연구

최상욱* · 채철주* · 김영호* · 이재광*

*한남대학교 컴퓨터공학과

A Study on Traceback System for Pharming Attack Response

Sang-wook Choi* · Cheol-joo Chae* · Young-ho Kim* · Jae-kwang Lee*

*Dept of Computer Engineering, Hannam University

E-mail : [suchoi, cjchae, yhkim, jklee]@netwk.hannam.ac.kr

요 약

기존의 침입 탐지 시스템이나 침입 차단 시스템과 같은 방어 시스템을 이용한 보안 정책은 중요 데이터와 자원을 관리함에 있어서 수동적 대응이라는 한계를 지니고 있다. 본 논문에서는 이러한 수동적 대응의 보안상 문제점과 한계성을 분석하고 대표적인 해킹 공격인 파밍 공격의 대응 방안과 해킹으로 판단되는 침입에 대해 ICMP 역추적 메시지(ICMP Traceback Message)를 이용한 ICMP기반 역추적 시스템을 설계한다. 본 연구를 통해 파밍 공격자의 근원지를 파악하고 최근 이슈가 되고 있는 개인정보 유출의 피해 방지와 금전적인 2차 범행을 사전에 차단 가능하다.

ABSTRACT

Security policy that use defense system such as Intrusion Detection System or Firewall is limited to passive response that only manage important data and resources. This paper analyzes security problem and maximum of passive response, provides a responsive way to Pharming attack which is one kind of hacking. This paper also includes ICMP-based traceback system that uses ICMP traceback Message about invasion that is decided through hacking. With this paper we can intercept damage of personal information leakage and property loss that is done through Pharming attacks.

키워드

Pharming, Traceback, 파밍, 역추적, iTrace

Ⅰ. 서 론

급속한 컴퓨터 네트워크의 발전과 더불어 해킹 기술 역시 콘솔 단위에서의 해킹에서 점차 자동화, 지능화, 분산화, 대규모화 되어가고 있다. 해킹의 목적 또한 자기만족과 흥미 위주의 단순 공격에서 금전적 이익을 노리는 전문 범죄로 변모해가고 있는 시점이고, 해킹의 기법은 날이 갈수록 지능화 돼 사용자의 도메인을 빼앗거나 도메인 네임 시스템 또는 프락시 서버의 주소를 변조하는 파밍(Pharming) 사이트까지 등장하게 되었다. 그러나 방화벽(firewall), 침입탐지시스템(IDS) 등과 같은 현재의 보안 관리 시스템은 침입자의 침입 시도 시 이를 탐지하고 방어하는 것이 주된 목적이기 때문에 이러한 파밍 공격에 대해 근본적인 해결책이 되지 않는다. 이와 같은 문제점을 해결하기 위해 공격자의 근원지를 파악하고 네트워크 접속 자체를 차단해 네트워크로부터 고립화 시키는 등 보다 능동적인 대응이 필요한 실정이다.

본 논문에서는 파밍 공격에 대해 실시간 역추적 기술을 적용한 능동형 보안 시스템을 제안하여 보다 안전한 네트워크 환경을 만들고자 한다. 본 논문의 구성은 2장에서는 파밍 공격과 능동적 대응 방법에 대한 관련 연구를 기술 하고, 3장에서는 침입자 역추적을 위한 IP 역추적 기법에 대

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행 되었음(IITA-2008-C1090-0801-0027)

해 소개하며, 4장에서는 침입자 역추적을 위한 능동형 보안 프레임워크를 기술한다.

II. 관련 연구

2.1 파밍(Pharming)

파밍 공격은 웹사이트 트래픽을 다른 웹사이트로 바꾸기 위한 공격의 일종으로써 잘 알려진 피싱 공격의 진화된 형태이다. 파밍 공격은 목표로 하는 피해 컴퓨터의 호스트 파일을 변경시키거나 DNS 서버 컴퓨터의 소프트웨어 취약성을 이용해 이루어진다. 파밍이란 용어는 farming과 phishing의 합성어로써 사용자명이나 비밀번호 등의 크리덴셜 정보에 접근하기 위한 사회 공학적 공격을 뜻한다. 이러한 파밍 공격은 피싱 공격보다 사용자가 알아차리기 더욱 어렵고 피해 규모 역시 비교가 불가능하기 때문에 각별한 주의를 필요로 한다. 대부분의 파밍 공격은 피싱 공격과 마찬가지로 새로운 해킹 기법이나 고도의 기술을 필요로 하지 않는다. 파밍은 일반적으로 DNS 캐시 중독, DNS 스푸핑, 도메인 하이제킹 등의 네임 서비스 취약성을 통해 발생되며, 국내의 많은 시스템 관리자들은 이런 도메인 네임 서버의 취약성에 대해 인지하지 못하고 있다. 그림 1은 도메인 네임 서비스의 취약성을 이용한 파밍 공격을 도식화 한 것이다.

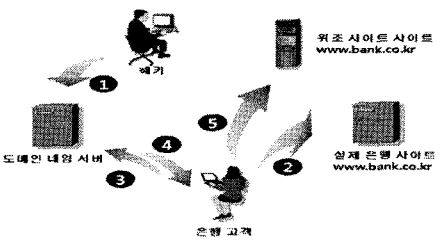

그림 1. 파밍의 공격 단계

먼저 해커는 www.bank.com 이라는 실제 은행 사이트를 해킹하기 위해 도메인 네임 서버의 버전을 확인하고 취약한 네임 서버의 상태를 확인 후, 공격을 시도하고 해당 시스템의 관리자 권한을 획득한다. 이러한 DNS 서버는 실제 은행 서버의 IP 주소를 포함하고 있고 공격자는 은행사이트의 IP를 위조한 시스템의 IP로 변경하게 되면 은행 사이트를 상시 이용하는 고객의 접근에 대해 사용자 시스템은 DNS 서버와의 질의, 응답을 통해 위조된 IP주소를 알려주게 된다. 그 후, 고객은 해커에 의해 위조된 시스템에 접속하게 되고 실제 사이트로 인식해 개인 및 금융 정보 등을 입력하게 된다. 이와 같은 순서를 거치게 되면 피해자는 의도하지 않은 정보를 유출하게 되고 유출 사실 또한 인식하지 못하게 된다.

보안상의 능동적 방어 기법이란 공격자의 침입 시도 시 이를 방어하고 탐지하는 것뿐만 아니라 역공격함으로써 공격자에게 피해를 입히는 적극적인 방어 기법을 의미한다. 능동적인 대응 기법은 역추적(traceback)과 트래픽에 대한 대응(blocking, isolation 등)에 주안점을 둔다. 따라서 능동적인 방어 기법이란 공격자를 역추적 하여 공격자의 근본적 위치를 발견하고 공격자 네트워크를 차단하는 등 보다 능동적인 형태의 대응 방법을 총칭한다[1].

III. IP 역추적 기법

3.1 네트워크 기반 역추적 시스템

네트워크 기반 역추적 기법은 네트워크상에서 송수신되는 패킷으로부터 역추적 정보를 얻어내어 공격자의 근원지를 파악하는 기법으로 송수신되는 패킷을 확인할 수 있는 위치에 설치된다. 이러한 역추적 기법에는 Hash-Based 역추적 기법인 SPIE(Source Path Isolation Engine)와 패킷 워터마크 기반의 SWT(Sleepy Watermark Tracing)등이 있다[2].

3.2 호스트기반 역추적 시스템

호스트기반 역추적 기법은 역추적을 위한 묘듈이 인터넷상의 모든 호스트에 설치되어 있다는 가정 하에 가능한 기법으로 호스트에서 발생하는 이벤트 로그 등의 다양한 정보를 바탕으로 역추적이 진행된다. 그러나 역추적 경로상의 일부 시스템에서 역추적 모듈이 설치되어 있지 않거나 어떤 문제 발생에 의해 역추적 정보를 얻을 수 없게 되는 경우가 발생하면 역추적이 불가능 하다는 단점을 가지고 있다. 이와 같은 문제점들로 인해 현재의 인터넷 환경에서 적용하는 것은 불가능하다[3].

3.3 패킷 마킹 역추적 시스템

패킷 마킹 역추적 기법은 연결된 네트워크를 순회하면서 지나간 라우터의 IP주소를 패킷 속에 삽입하는 방식으로 마킹된 패킷을 받은 호스트는 라우터 주소 정보를 이용하여 지나온 경로를 구성할 수 있게 한다. 일반적으로 패킹 마킹은 TCP/IP 프로토콜 중에서 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[4][5].

IV. 파밍 공격 대응 보안 시스템 설계

파밍 공격 유형은 매우 광범위 하고 다양하기 때문에 본 논문에서는 DNS 서버 공격에 대한 실시간 대응 방법으로 범위를 제한 한다. 일반적으로 파밍 공격자는 최종 희생 시스템(DNS 서버)에 침입하기 전에 여러 단계의 중간 경유 호스트를

이용하게 된다. 이러한 과정에서 중간 경유지 호스트에는 침입자의 침입을 나타내는 각종 이벤트 로그가 기록되어지며, 추후 로그분석을 이용해 역추적이 가능하도록 한다. 그러나 대부분의 전문적 침입자들은 경유지의 로그기록을 삭제하는 등 흔적을 남기지 않게 되고 이는 곧 역추적이 불가능하다는 것을 의미하게 된다. 따라서 본 논문에서는 침입자의 공격 시도 시 실시간으로 침입자 역추적이 가능한 메커니즘을 제안하고 있다.

본 논문에서 제안하는 실시간 보안 시스템 프레임워크는 IP 역추적을 위하여 IETF가 제안하는 iTrace Message(ICMP Traceback Message)를 이용하며, 각 지역 네트워크 및 관리 네트워크에 에이전트와 서버를 설치한다. 각 지역 네트워크에 설치된 에이전트는 역추적 시 iTrace Message를 생성하여 서버에 전송하게 되고 관리 네트워크에 설치된 서버는 각 지역 네트워크에 설치된 에이전트들로부터 수신한 iTrace Message를 이용하여 침입자 역추적을 수행하게 된다. 그림 2는 본 논문에서 제안한 역추적 시스템 서버와 에이전트가 설치된 네트워크의 구조이다.

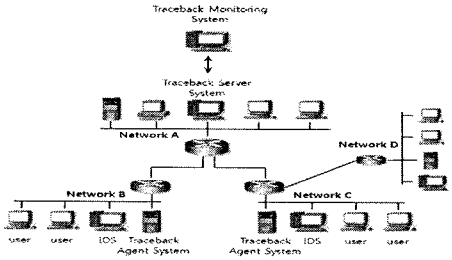

그림 2. 역추적 서버/에이전트가 설치된 네트워크 구조

4.1 iTrace Message 구성

본 논문에서 제안한 iTrace Message의 구조는 그림 4와 같은 형태를 가지고 있다. 메시지는 ICMP 형태인 ICMP 패킷을 전달한다.

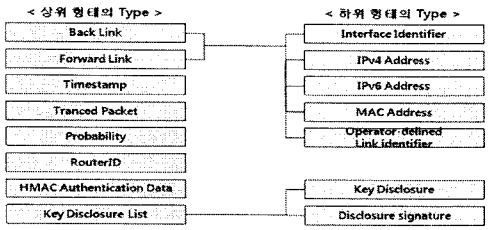

그림 3. ICMP Traceback Message 구성

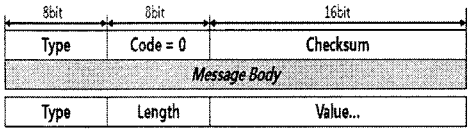

그림 4. ICMP Traceback Message 형태

iTrace Message는 반드시 하나의 Forward Link elemet 또는 Back Link element를 포함해야만 한다. 각 Lint elemet는 traced 패킷의 이동경로 및 공격자 출발지에 대한 정보를 제공하고 iTrace Message 연결 구성을 위한 경로 정보를 제공하게 되고 Message의 위변조를 방지하기 위해 전자서명 인증 기술인 SHA-1을 사용해 구현한다.

4.2 에이전트 시스템 설계

에이전트는 각 지역 네트워크에 설치되어 네트워크 트래픽 수집, 패킷 분석, iTrace Message 탐지, 생성, 비정상 패킷 처리 등을 수행하게 된다.

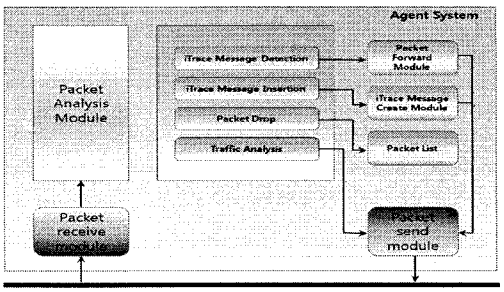

그림 5. 에이전트 시스템 구성

역추적 경로 정보를 담고 있는 iTrace Message는 패킷들로부터 확률적인 패턴 추출이 가능하기 때문에 침입 공격에 대하여 실시간적이고 능동적인 대응 능력을 가지고 있다. 이러한 iTrace Message의 생성 및 검증 절차는 먼저 공격자에 의한 위변조를 방지하기 위해 서버와 에이전트는 비밀키를 공유한다고 가정한다. 최초 서버측은 난수 생성기를 이용하여 비밀키(K)를 생성하고 비밀키 DB에 저장한다. 그다음 생성된 비밀키를 에이전트와 공유하고 에이전트는 iTrace Message 생성 모듈을 이용하여 iTrace Message를 생성한 후 공유한 비밀키(K)와 해시함수(SHA-1)을 이용하여 iTrace Message를 생성한다. 이렇게 해서 생성된 iTrace Message와 해시값을 에이전트는 서버에 전송하고 서버는 공유한 비밀키(K)를 이용하여 iTrace Message 해시값을 생성한 후 에이전트로부터 전송된 iTrace Message 해시값과 비교하고 만약 일치 한다면 역추적 경로 구성 모듈로 전송한다.

4.3 서버 시스템 설계

서버는 관할 네트워크의 현황을 실시간으로 모니터링 해주는 기능과 에이전트와 서버간의 네트워크 관리 정보 교환을 통해 유기적인 공격탐지 및 대응 프로세스 처리가 가능하도록 설계하였다.

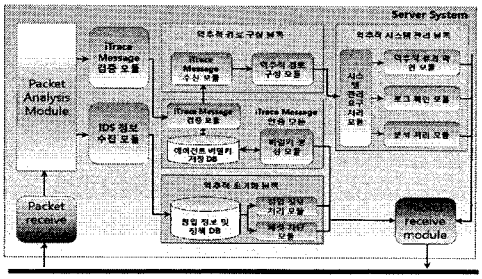

그림 6. 서버 시스템 구성

서버 시스템은 에이전트로부터 수신한 iTrace Message를 검증하기 위해 iTrace Message 인증을 사용하고 공격자에 의해 위변조된 iTrace Message를 식별한 후 폐기 유무를 결정한다.

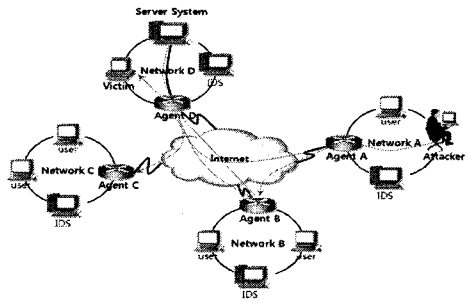

그림 7. 공격에 대한 역추적 대응 과정

그림 7은 본 연구에서 설계된 해커의 공격에 대한 역추적과 대응, 그리고 역추적 결과를 통보하는 메커니즘을 보여주고 있다. 서버와 에이전트는 비밀키를 서로 공유하고 있고 역추적을 위한 에이전트는 라우터나 AP에 모듈화 되어 있다는 가정 하에 모든 패킷에 대해 1/20,000의 확률로 iTrace Message를 생성한다.

네트워크 A내의 해커가 네트워크 D에 존재하는 DNS 서버를 공격한다면 다음과 같은 역추적 과정을 거쳐 대응하게 된다

단계 1. 네트워크 A내의 해커는 네트워크 D에 존재하는 서버를 공격하기 위해 네트워크 B를 경유한다.

단계 2. 해커가 네트워크 D에 존재하는 DNS 서버에 대해 공격 시도한다.

단계 3. 네트워크 D의 라우터는 공격 탐지 후 침입 사실을 서버로 통보한다.

단계 4. 서버는 침입 사실을 네트워크 D내의 다른 에이전트들에게 전달한다.

단계5. 서버는 각 에이전트들로부터 수신한 iTrace Message의 유효성 검증을 이전에 공유한 비밀키(K)를 이용하여 실시한다.

단계 6. 서버는 수신한 iTrace Message 중에서 Timestamp 값이 가장 큰 iTrace Message를 선택하여 RouterID에 대한 backward link와 forward link를 저장한다.

단계 7. backward link와 일치되는 forward link를 가진 iTrace Message 중에서 timestamp 값이 가장 차이가 적은 iTrace Message를 선택하여 연결 체인을 형성한다.

단계 9. 서버는 공격자 근원지를 파악하여 공격자에 대해 네트워크로부터의 단절 정책을 결정한다.

V. 결 론

인터넷을 이용한 금융 거래가 급속하게 증가함과 동시에 이를 노리는 해커들의 공격 또한 점점 지능화 되고 발전하는 추세이다. 피싱 공격의 진보된 형태인 파밍 공격은 호스트를 직접 공격 할 뿐만 아니라 DNS 서버 공격이나 라우터의 라우팅 테이블 정보를 직접적으로 변경하는 등 피해의 규모가 날로 거대해지고 있다. 본 논문에서는 파밍 공격의 유형 중 하나인 DNS 서버 공격에 대한 탐지뿐만 아니라 적극적이고 능동적인 역추적 시스템을 설계 및 구현하였다.

향후 연구로는 본 논문에서 제안한 역추적 시스템을 바탕으로 라우터 및 AP 공격에 대한 역추적 시스템과 더 나아가 무선 네트워크 환경에서 발생 가능한 공격에 대해 능동적인 역추적 시스템 연구가 필요하다.

참고문헌

[1] 단행본: "차세대 인터넷을 위한 능동 보안 기술 백서", 한국전자통신연구원, 2001

[2] 서동일, "패킷 워터마크 기반의 인터넷 침입자 실시간 연결 역추적 메커니즘", 충북대학교 대학원 이학박사학위논문, 2004

[3] H. T. Jung et al. "Caller Identification System in the Internet Environment", 4th Usenix Security Symposium, 1993.

[4] 강동호, 한승완, 서동일, 장종수, "IP 역추적 기술 동향", 주간기술동향, 97-39 한국전자통신연구원

[5] D. X. Song, A. Perrig, "advanced and Authenticated Marking Scheme for IP Traceback", Proc. Infocom Vol2, pp 878-886, 2001