침입탐지 모듈을 이용한 역추적시스템 개발

김 선 영*°, 구 향 옥*, 서 동 일**, 오 창 석*
충북대학교*
한국전자통신연구원**

Development of Traceback System Using IDS Module

Kim sun-young*°, Koo hyang-ohk*, Seo dong-il**, Oh chang-suk*
Chungbuk National Univ.*
Electronics and Telecommunications Research Institute**
E-mail : sykim@nwork.chungbuk.ac.kr

요 약

본 논문에서는 크래커가 여러 곳의 시스템을 경유하여 침입을 하였을 경우, 크래커의 경로를 역추적하기 위한 효율적인 역추적 모델을 제안하고 구현하였다. 구현한 역추적 시스템은 역추적 서버 모델, 역추적 클라이언트 모델로 구성된다. 역추적 클라이언트는 에이전트가 설치된 곳에서 침입관련 정보를 역추적 서버로 전송하여 크래커가 침입의 경유지로 어느 시스템을 이용하였는지를 판별한다. 구현한 역추적 시스템으로 클라이언트 에이전트가 설치된 곳에서는 효율적인 역추적 경로를 추적할 수 있었다.

Abstract

A system connected in Internet can be intruded by cracker via several systems. This paper proposes an efficient traceback model in order to trace a route of crackers. The traceback system is composed of a traceback server model and a traceback client model. As transmitting intrusion information from an area where client agent is installed to traceback server, the system distinguishes which systems are used as intrusion route. The traceback system can retrace intrusion route efficiently in an area where a traceback client is installed.

I. 서 론

최근에 인터넷을 이용한 새로운 유형의 크래킹 기법들이 지속적으로 출현하고, 이에 따른 피해도 점차 확대되고 있는 실정이다. 따라서, 크래커들의 크래킹을 차단함으로써 시스템을 보호하는 것은 매우 중요하게 되었다. 최근에 크래킹을 차단하기 위한 다양한 기법들이 개발되고 있으나 현실적으로 모든 공격을 방지하는 것은 어렵기 때문에 크래커를 조기 검출하여 피해를 최소화하는 방안을 연구하는 것이 시급한 실정이다.[1][2]

본 논문에서는 역추적시스템 구축을 위해 역추적 서버와 역추적 클라이언트로 구성된 실시간 역추적 시스템 모델을 제안하였다. 역추적 클라이언트는 침입탐지 규칙을 적용하여 네트워크에 흐르는 패킷 중에서 부정한 패킷을 추출하고, 이 패킷 헤더 부분의 내용을 분석하여 역추적할 수 있는 근거가 되는 내용이 있으면 역추적 서버에 보고한다. 역추적 서버는 클라이언트가 보고한 내용을 분석하여 역추적 할 수 있는 경로 정보를 추출하

고, 역추적 하는 과정과 역추적 결과를 웹 환경에서 실시간으로 보여준다.

본 논문에서 제안하고 구현한 역추적 시스템은 빈번한 크래커의 크래킹을 검출하고, 크래커를 감소시킬 수 있는 매개체가 될 것이다.[3]

II 실시간 역추적 시스템 설계

1. 실시간 역추적 서버 모델 설계

실시간 역추적 서버 시스템 구조는 그림 1과 같이 6개의 서브 모듈로 구성되어 있다. 역추적 요구부는 패킷을 캡쳐하고, 분석하는 과정 중 어떤 특정한 역추적 클라이언트에 침입 경보가 발생할 경우, 역추적 클라이언트에 있는 Snort로부터 패킷 헤더의 정보를 분석한 침입 탐지 정보를 요구한다. 역추적 분석부는 요구부로부터 전송된 역추적 클라이언트들의 침입 관련 데이터와 역추적 서버에서 캡쳐한 패킷 헤더의 침입 탐지 정보를 가지고 역추적 서버시스템의 분석부에서 크래커가 어떤 크래킹 수법으로 침입하였는지 비교한 결과를 정보 인출부로 전송한다. 정보 인출부는 분석부로부터 받은 분석된 침입 관련 데이터와 역추적 경로 정보부로부터 전송 받은 경로 정보 관련 데이터를 PHP 기반의 응용 프로그램인 ACID로 보낸다.[4]

역추적 경로 정보부는 분석부로부터 받은 패킷 헤더의 정보를 분석하여 정보 인출부로 전송하고, 데이터를 저장한다. 역추적 상황 보고부는 경로 정보부로 부터 받은 침입 관련 데이터를 Snarf로 보낸다. 정보 저장부는 역추적 경로 정보부로부터 받은 정보를 각각의 데이터 베이스 테이블에 정렬해서 저장하고, 요구시 전송해 주는 모듈이다.[5]

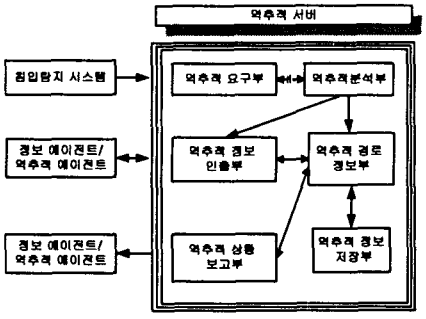


그림 1. 역추적 서버 구조

2. 실시간 역추적 서버 시스템의 흐름도

실시간 역추적 서버 시스템에 의심스러운 패킷이 들어올 경우는 그림 2와 같이 크게 3가지 경우로 분류된다.

■ 의심스러운 패킷을 캡쳐 후 패킷 규칙 집합에 적용하여 규칙 집합과 패턴이 일치하면 패킷 분석부로 보낸다. 패킷 분석부에서는 패킷을 정밀 분석하여 침입이 아닌 경우 정상 패킷으로 판정하여 패킷을 버리고 종료한다.

■ 의심스러운 패킷을 캡쳐 후 패킷 규칙 집합에 적용하여 규칙집합과 패턴이 일치하지 않으면 다른 규칙집합과 패턴매칭을 한다. 만약 다른 규칙집합과 패턴이 일치하면 패킷 규칙 집합으로 리턴한 후 패킷 분석으로 이동하여 위 두 가지 경우를 수행하는 경우이다.

■ 의심스러운 패킷을 캡쳐 후 패킷 규칙 집합에 적용하여 규칙 집합과 패턴이 일치하지 않고 다른 규칙 집합과도 패턴이 일치하지 않다면 정상 패킷으로 간주, 패킷을 버리고 종료하는 경우이다.

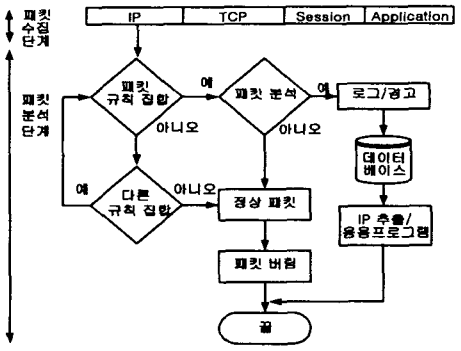


그림 2. 실시간 역추적 서버 시스템 흐름도

3. 실시간 역추적 클라이언트 시스템 설계

실시간 역추적 클라이언트 시스템의 구조는 역추적 정보 수집부, 역추적 분석부, 역추적 상황 보고부, 역추적 클라이언트 시스템 연결부로 구성되어 있다. 그림 3은 실시간 역추적 클라이언트 시스템의 구조를 나타낸 것이다.

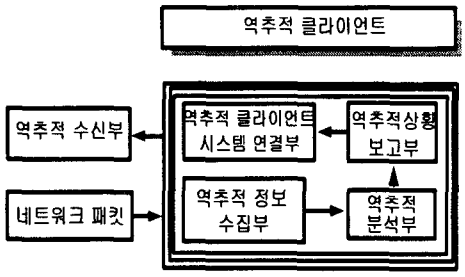


그림 3. 실시간 역추적 클라이언트 시스템 구조

■ 역추적 정보 수집부

역추적 정보 수집부는 실시간 역추적 클라이언트 시스템의 입력부로서 실시간 역추적 클라이언트 시스템을 통과하는 모든 네트워크 패킷 중 의심스러운 패킷을 수집하여 역추적 클라이언트 분석부로 전송한다.

■ 역추적 분석부

역추적 정보 수집으로부터 받은 의심스러운 정보를 가지고 크래커의 크래킹 유형과 포트번호, IP를 분석하여 역추적 상황 보고부로 전송한다.

■ 역추적 상황 보고부

역추적 상황 보고부는 역추적 분석부에서 분석된 정보를 바탕으로 크래킹 유형에 맞는 규칙 집합에 적용하고 침입 여부를 판정하여 역추적 클라이언트 시스템 연결부로 전송하다.

■ 역추적 클라이언트 시스템 연결부

역추적 상황 보고부에서 받은 모든 침입 탐지 정보를 전송 받아 실시간으로 역추적 서버 시스템의 수신부와 접촉하여 침입 탐지 정보를 전송한다.

Ⅲ 역추적 시스템의 시험 및 결과 고찰

1. 시험 시스템의 구성

시험은 LAN을 이용한 시험망을 사용하였으며 그림과 같이 망을 구성하였다. 한편, 본 시험에 사용된 시험망의 구성 환경은 PentiumⅢ이상의 서버 1대, 클라이언트 2대와 100Mbps의 스위칭 허브에서 실험하였다. 시험 환경은 그림 4과 같다.

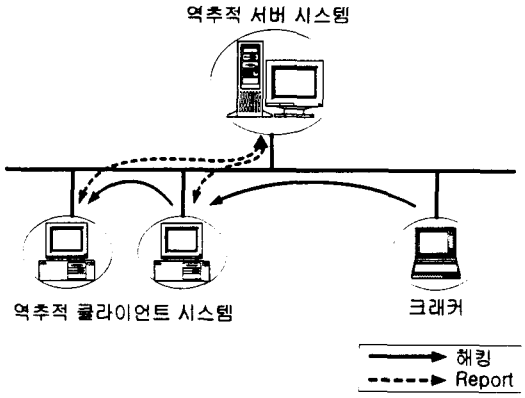


그림 4. 시험 환경

2. 시험 내용 및 결과 고찰

본 논문에서 제안하고 구현한 실시간 역추적 시스템에서는 크래커가 경유지를 통해 역추적 클라이언트 시스템들을 크래킹하게 되면 역추적 클라이언트 시스템들은 침입 관련 데이터를 역추적 서버 시스템에 전송한다. 역추적 서버 시스템에서는 역추적 클라이언트로부터 전송된 데이터를 분석한 후 역추적 서버 시스템에 로깅된 데이터와 클라이언트의 데이터를 비교, 분석하여 크래커를 역추적하는 환경을 구축하여 테스트하였다. 실시간 역추적 서버 시스템의 메인 화면은 그림 5를 통해서 크래커가 경유하게될 클라이언트 시스템의 배치를 알 수 있다.

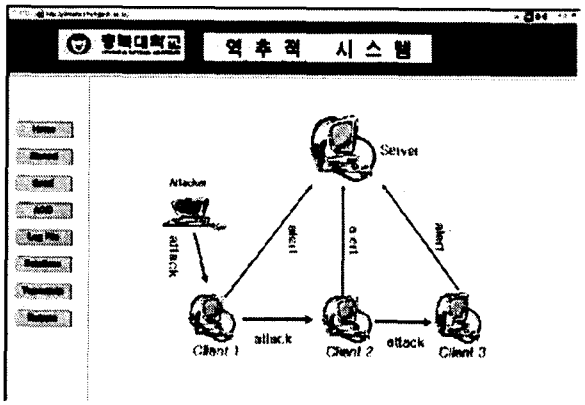


그림 5. 실시간 역추적 시스템 메인 화면

그림 6은 역추적 서버 시스템에서 생성된 로그들의 목록을 보여주고 있다. 역추적 서버 시스템의 관리자가 필요하다고 생각되는 시스템 로그들을 추가할 수 있으

며, 로그 목록으로는 역추적 클라이언트들의 로그파일과 역추적 서버에서 생성된 경고 로그 파일 등이 있다. 원하는 로그를 클릭하게 되면 역추적 서버 시스템에서 생성된 세부 내용을 알 수 있다.

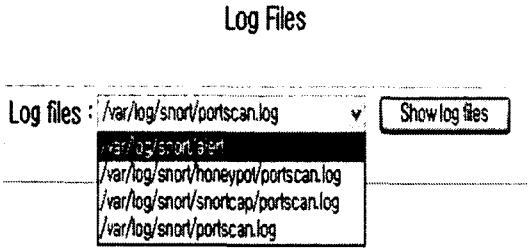
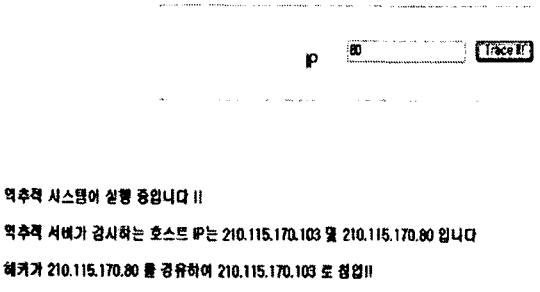


그림 6. 실시간 역추적 시스템 로그 목록 화면

그림 7의 a는 역추적 서버 시스템에서 설정된 시간외에 추적을 하였을 경우와 로컬 시스템이 아닌 외부 시스템을 입력하였을 때 실행한 화면을 나타낸다. 그림 7의 b는 역추적 서버 시스템에서 역추적 클라이언트 시스템인 X.X.X80번을 경유하여 크래커가 침입하였을 때를 각각 보여주고 있다.

(a) 최종 경로 화면



(b) 최종 경로 화면

그림 7. 실시간 역추적 시스템 최종 경로 화면

Ⅳ.결 론

본 논문에서 제안한 실시간 역추적 시스템 모델은 크래커의 경유지 주소를 클라이언트 에이전트가 설치된 곳에 한하여 알아낼 수 있다. 크래커의 근원지 주소는 현재까지 전 단계 에이전트로 이동하는 문제 때문에 알아내기가 쉽지 않을뿐더러 결국 또다른 크래킹을 해야하는 윤리적 문제를 파생시킨다.

본 논문에서 제안하고 구현한 역추적시스템은 크래커를 역추적하기 위해서 전 단계로 이동하지 않아도 의심스런 패킷 헤더를 분석하거나 클라이언트 시스템에서 역추적 서버로 전송해온 침입 관련 로그파일을 분석하여 역추적 함으로써 클라이언트 에이전트가 설치된 곳에 한하여 크래커의 침입탐지와 경유지를 알아낼 수 있었다. 이 시스템을 전체 네트워크로 확장한다면 해커의 경유지 뿐만 아니라 근원지를 파악하는데 크게 기여할 수 있을 것으로 추정한다.

참 고 문 헌

[1] Eugene H. Spafford, Diego Zamboni, "Intrusion detection using autonomous agents", 2000 Elsevier Science B.V.

[2] 정연서, "정책기반의 멀티에이전트 침입 탐지 메커니즘", 2001.8

[3] 오창석, 데이터통신, 영한출판사, 1999

[4] 임채호, "인터넷 해킹 기법을 이용한 실용적인 크래커 추적 기술에 관한 연구", 2000.12

[5] 한국정보보호센터 송주석, 강명호, 김수형, 조형재, "전산망 시스템 크래커 역추적 기본시스템 개발", 1997