ISSN 1738-7531

보안공학연구논문지
JSE

Journal of Security Engineering

Vol. 9, No. 6, December 2012

보안공학연구지원센터

보안공학연구논문지
Journal of Security Engineering

ISSN : 1738-7531 제9권,제6호,2012년12월

목 차

자동화 침입탐지 데이터베이스 시스템의 개발

신상윤[1], 장원태[2], 연규철[3], 김영철[4]

Database System of Automated Intrusion Detection

Sang-Yoon Shin[1], Won-Tae Jang[2], KyuChul Yeon[3], R. Young Chul Kim[4]

요 약

정보화가 발달 되면서 해당 정보를 불법적으로 얻기 위한 많은 시도들이 발견되고 있다. 이에 따라 서비스 업체들은 다양한 침입 탐지 시스템을 개발하고 있다. 우리도 패턴 데이터베이스화를 통해 매칭 기법을 이용하여 직접 구현하였다. 그리고 침입 발생시 APP 알림 메시지를 전달하여 주는 기능도 구현하였다. 또한 확장성을 고려하여 탐지 패턴을 관리하는 인터페이스도 구현 하였다.

핵심어 : 침입 탐지 시스템, 데이터베이스, 패턴 매칭

Abstract

It has found many trials to gain important information with illegal way as advanced information systems. Some security service companies develop various intrusion detections. To easily manage intrusion detection, we implement pattern database system through pattern mapping technique, and also develop App for alarm message to send alarm when someone tries to do intrusion. To consider extension, we also implement interface to manage detection pattern.

Keywords : Intrusion Detection, Database, Pattern matching

1. 서론

현재 많은 서비스업체들은 악의적인 목적을 가진 침입자에 의해 정보 접근시도를 당하고 있고

접수일(2012년10월02일), 심사의뢰일(2012년10월04일), 심사완료일(1차:2012년10월12일, 2차:2012년10월25일)
게재일(2012년12월31일)

[1]339-701 세종특별자치시 조치원읍 세종로 2639 홍익대학교 컴퓨터정보통신공학과.
email: loossye@gmail.com

[2]339-701 세종특별자치시 조치원읍 세종로 2639 홍익대학교 컴퓨터정보통신공학과.
email: wtjang0609@naver.com

[3]339-701 세종특별자치시 조치원읍 세종로 2639 홍익대학교 컴퓨터정보통신공학과.
email: 70m4.kyuf3@gmail.com

[4](교신저자) 339-701 세종특별자치시 조치원읍 세종로 2639 홍익대학교 컴퓨터정보통신공학과.
email: bob@selab.hongik.ac.kr

* 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업(2012-0001845)과 교육과학기술부와 한국연구재단의 지역혁신인력양성사업으로 수행된 연구결과임.

이를 막기 위해 다양한 침입탐지 솔루션들을 사용하고 있다. 침입탐지 방법에도 여러 가지가 있는데 대표적으로 오용탐지, 이상탐지가 있다. 오용탐지는 침입 행위를 먼저 명시하고 이와 같은 방식의 접근을 허용하지 않는 방법으로 백신프로그램에서 사용하는 방법과 같다. 이상탐지는 정상적인 흐름이 깨질 때 탐지하는 방법인데 구현비용도 크고 현재 완벽하게 구현된 시스템은 없다.

본 논문에서는 이런 두 가지 방식의 장점만을 취한 하이브리드 방식의 탐지방법을 구현하고자 한다. 사용자가 직접 패턴을 입력하는 오용탐지 방식과 시스템의 로그를 이용하여 이상탐지 부분을 찾아내고 시스템이 이를 수정해 주도록 하였다. 이에 대해서는 본문에서 자세히 설명하도록 하겠다.

본 논문의 구성은 다음과 같다. 2장에서 관련 논문에 대해 설명을 하고 3장에서 이를 이용한 본 논문의 결과를 설명한다. 마지막으로 4장에서 향후 발전 방향을 언급한다.

2. 관련연구

2.1 오용 탐지

침입행위를 미리 자료화 하고 이를 기반으로 탐지하는 기법이다. 그렇기 때문에 탐지에 기반이 되는 침입행위의 자료가 먼저 필요하다. 그러나 알려진 기법들에 대한 탐지는 우수하다. 하지만 새로운 기법의 공격에는 취약하며, 오탐지를 줄이기 위해서는 세밀한 패턴의 자료가 필요하다.

2.2 이상 탐지

침입자의 어떤 불법적 행위가 시스템의 정상 동작과 일치하지 않음을 탐지하는 기법이다. 이 기법은 시스템에서 발생되지 않아야 할 에러가 탐지되거나 의도되지 않은 행동을 탐지한다. 이는 알려지지 않은 의외의 공격에 대해 강한 장점을 가지나 구현비용이 매우 크고 실제로 완벽하게 구현된 시스템은 존재하지 않는다. 또한 장기간의 학습이 필요하며 오탐지율이 높아 관리자가 관리가 어렵다.

3. 자동화 침입탐지 시스템 설계

3.1 요구사항

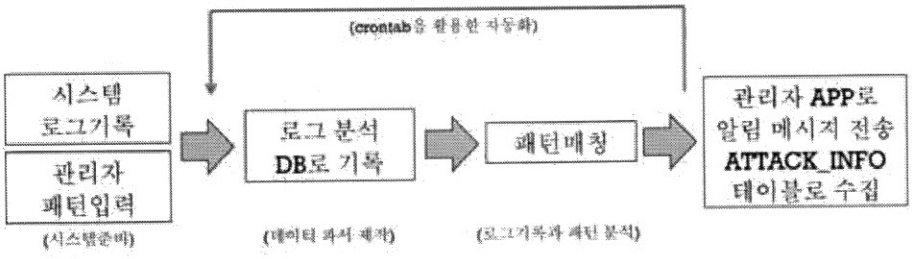
본 논문에서는 오용탐지, 이상 탐지 두 가지 방법의 장점만을 이용한 hybrid 방식의 탐지를 이용할 것이다. 실제로 하이브리드 방식의 탐지는 대다수의 탐지 시스템에서 이용하고 있는 것으로 오용탐지는 간단한 패턴을 자료화하여 입력하고 이를 전문가가 세밀한 패턴을 정의 하면 시스템이 이를 기반으로 이상탐지를 하는 방식이다.

우리는 기존의 방법과 비슷하지만 조금 다르게 구성하였다. 제안한 방법은 시스템이 작성한 로그를 기반으로(이상탐지) 이 로그의 정보를 전문가가 패턴화하고 이를 매칭시키는(오용탐지) 방법을 이용하여 실 시스템의 자원을 활용하여 간단하고 쉽게 바로 적용시킬 수 있는 솔루션을 제작한다. 이 솔루션의 요구사항은 아래와 같다.

- 해킹 공격 기술을 데이터베이스로 만들어 공격이 들어오면 사용자에게 알려준다.
- 로그에는 로그 종류, 로그 시간, 공격자 IP 정보, 보유한 서버들의 IP 정보 공격자가 공격한 코드내용이 들어간다.
- 서버 정보에는 서버 IP, 서버이름, 사용 목적, 서버 OS 의 정보가 있다.
- 공격한 정보에는 공격자의 IP, 서버 IP, 공격기술이 필요하다.
- 공격 기술들은 공격 기술의 종류, 기술의 이름, 공격 코드 템플릿이 있다.
- 날짜, 공격자, 서버 별 각각 어떤 공격이 들어왔는지 통계를 내준다.

3.2 설계

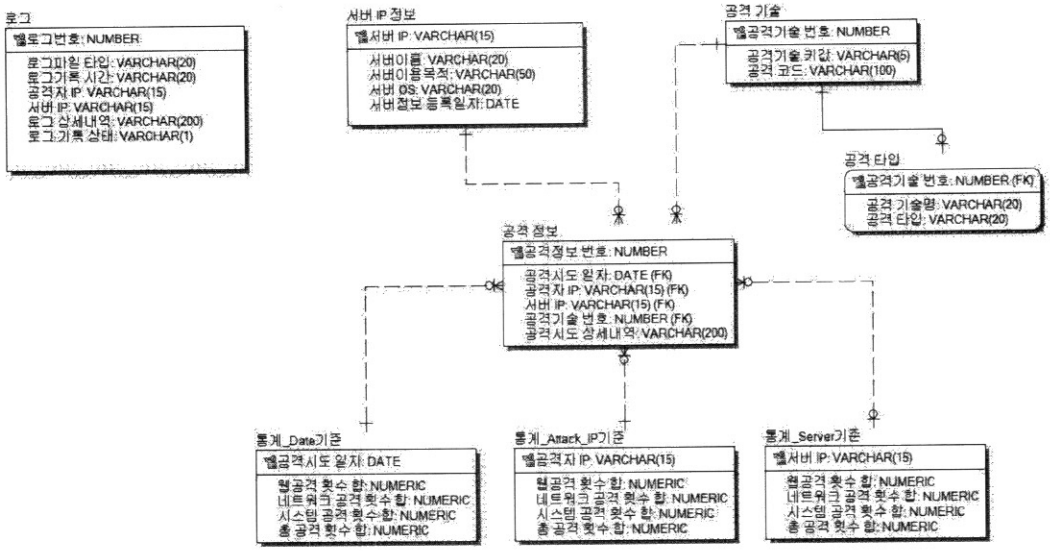
시스템의 로그파일과 관리자가 입력할 자료의 패턴들을 준비하여 시스템을 구성한다. 각 로그별로 기록 방식이 다르므로 로그별 파서를 제작한다. 제작방법은 로그들은 공백를 구분자로 기록하므로 이를 이용하여 DB에 구분하여 저장한다. DB에 기록된 로그들과 관리자가 입력한 패턴을 활용하여 패턴매칭하여 공격유무를 판단한다. 공격으로 판단되면 해당 정보를 사용자에게 알려주고 이를 다시 정보화하기 위하여 ATTACK_INFO 테이블로 재 저장한다. [그림 1]은 자동화 침입탐지 시스템의 알고리즘을 도식화한 것이다.



[그림 1] 자동화 침입탐지 시스템의 알고리즘

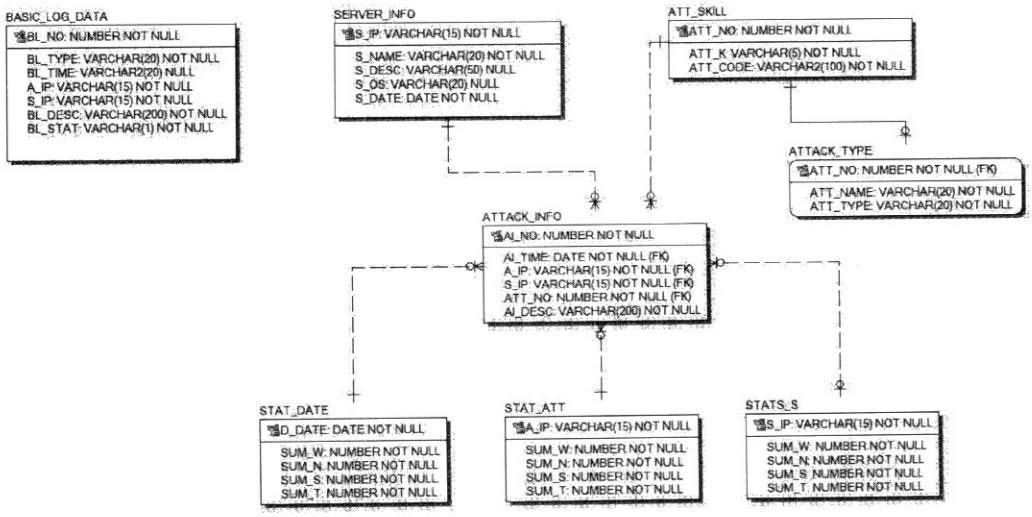
[Fig. 1] Algorithm of automatic Intrusion Detection System

자동화 침입탐지 시스템의 데이터를 저장하기위해서 로그 기록은 데이터베이스에 저장해야한다. [그림 2]와 [그림 3]은 로그 기록을 위한 데이터베이스의 논리적 물리적 설계 결과이다.



[그림 2] 논리적인 데이터베이스 설계

[Fig. 2] Design of logical databases



[그림 3] 물리적인 데이터베이스 설계

[Fig. 3] Design of physical databases

4. 자동화 침입탐지 시스템 구현

4.1 로그 파서

- 각 로그별로 기록 방식이 다르므로 로그별 파서를 제작한다.
- 구분자는 공백(스페이스바)를 이용하고 아래와 같이 [기록시간], [공격 IP], [대상 IP], [공격코드]의 위치가 모두 다르므로 이를 분리하여 DB로 일정하게 입력한다.

Error_log

```
[Mon Apr 30 00:56:48 2012] [notice] child pid 11603 exit signal Segmentation fault (11)
[Mon Apr 30 00:56:58 2012] [notice] SIGHUP received.  Attempting to restart
[Mon Apr 30 00:56:58 2012] [notice] Apache/2.2.8 (Unix) PHP/5.2.9 configured -- resuming normal operations
```

Access_log

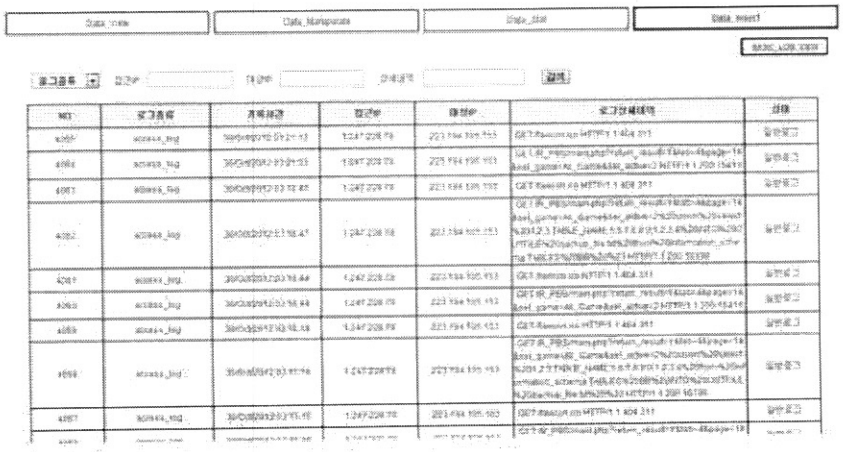
```
1.247.228.78 - - [31/Oct/2012:12:26:57 +0900] "GET /favicon.ico HTTP/1.1" 404 209
1.247.228.78 - - [31/Oct/2012:12:27:05 +0900] "POST /~WEB_TEST/R_PBS/main.php?tab=99&page=96 HTTP/1.1" 200 3476
1.247.228.78 - - [31/Oct/2012:12:27:05 +0900] "GET /~WEB_TEST/R_PBS/css/style.css HTTP/1.1" 304 -
```

[그림 4] 시스템의 로그 데이터

[Fig. 4] log data of system

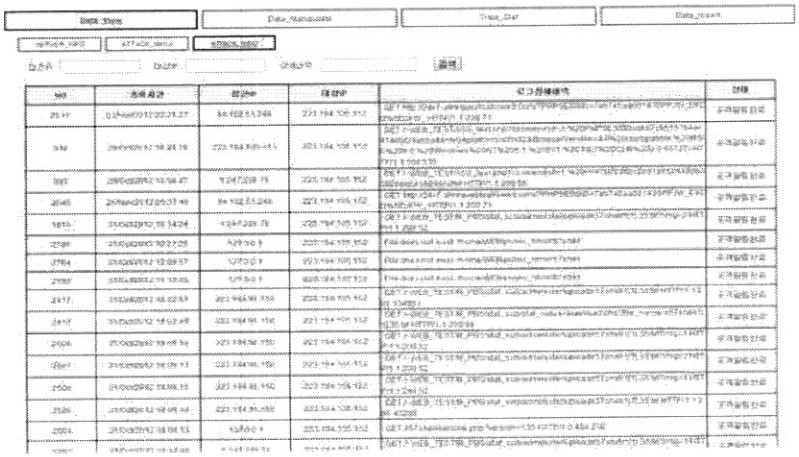
4.2 웹 인터페이스

- [서버관리], [공격패턴관리] 등의 관리 메뉴가 존재 한다.
- 순수하게 수집된 각 로그 데이터를 보여주고 이를 패턴 매칭 하여 공격 판별된 로그를 보여준다.
- 관련 통계 자료를 제공한다.



[그림 5] 수집된 로그 데이터

[Fig. 5] collected log data



[그림 6] 공격이 판별된 로그

[Fig. 6] Log to determine the attack

4.3 안드로이드 APP 테스트

- 안드로이드 어플리케이션을 이용하여 서버정보와 패턴확인을 하고 해당 정보의 입력기능을 제공한다.
- 침입탐지가 방생하였을 때 Notification을 이용하여 사용자에게 알림 메세지를 주고 해당 로그 기록을 보여준다.

[그림 7] 안드로이드 어플리케이션의 테스트

[Fig. 7] Test of Android Application

5. 결론

본 논문에서는 기존의 탐지방법의 장점을 모은 hybrid 방식의 탐지 방법을 제안하였다. 제안한 방법은 오용탐지와 이상탐지부분을 기존의 방법과 다르게 변경하였다. 변경한 이상탐지는 시스템에서 생성한 로그 데이터들을 기반으로 관리자가 패턴매칭을 사용하여 오용을 탐지하는 방법이다. 두 장점을 이은 이 방법을 솔루션으로 개발 할 수 있었고 보다 손쉽고 편리한 방법으로 여겨진다.

본 논문에서는 로그 파싱을 웹기반으로 제작하였는데, 이것은 시스템 로그 및 FTP 서비스 등의 로그들로 확장시킬 수 있어 이식성이 좋다. 향후에는 각 로그별 파서들을 제작하고 이를 기반으로 웹 공격뿐만 아니라 시스템 전반에 걸친 탐지가 가능한 방법을 연구중이다. 이를 고려하여 관리자의 패턴 입력 역시 웹, 시스템, 네트워크 등 여러 공격 패턴이 입력 가능하도록 고려하고 있다.

사용성을 위해서는 해당 웹 UI에서 공격 코드부분의 강조라던가 웹에서도 Ajax를 이용한 비동기식 알림을 제작하여 모니터링 요원의 피로도를 덜어줄 수 있는 방법도 고안될 수 있을 것이다.

참고문헌

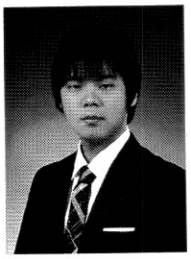
[1] 박대우, 임승린, "해커의 공격에 대한 지능적 연계 침입방지시스템의 연구", 한국컴퓨터정보학회지, 제 11권 제 2호, pp.351-360, 2006. 5.

[2] 강상원, 이하용, 양해술, "침입방지 시스템의 보안성 품질평가 모델 개발", 제 32 회 한국정보처리학회 추계학술발표대회, 2009.

저자 소개

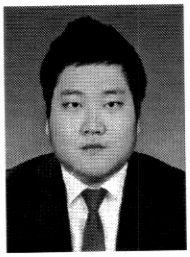
신상윤 (Sang-Yoon Shin)

2010년 2월~현재 : 홍익대학교 과학기술대학 컴퓨터정보통신 재학중
2011년 : 홍익대학교 정보 보안 동아리 H.U.S.T 12th 회장
관심분야 : 컴퓨터 보안



장원태 (Won-Tae Jang)

2007년 2월~현재 : 홍익대학교 과학기술대학 컴퓨터정보통신 재학중
관심분야 : 컴퓨터 보안



연규철 (Kyu-Chul Yeon)

2007년 2월~현재 : 홍익대학교 과학기술대학 컴퓨터정보통신 재학중
2012년 : 홍익대학교 정보 보안 동아리 H.U.S.T 13th 회장
관심분야 : 컴퓨터 보안

김영철 (R. Young-Chul Kim)

2000년 : Illinois Institute of Technology(공학박사)
2000년~2001년 : LG 산전 중앙연구소 Embedded system 부장
2001년~현재 : 홍익대학교 컴퓨터정보통신 교수
관심분야 : 테스트 성숙도 모델(TMM), 임베디드 소프트웨어 개발 방법론, 모델 기반 테스팅, 메타모델, 비즈니스 프로세스 모델, 사용자 행위 분석 방법론