트레이스 라우트 정보와 접속 통계 정보를 이용한 원격지 접속 오탐율 개선 모델 설계

백현철*, 김상복**, 김창근***

요약

오늘날 기업에서는 업무의 신속성을 위하여 인터넷과 인트라넷 등 네트워크를 기반으로 하여 모든 업무를 운영하고 있다. 특히 새로운 원격지로부터 접속해 오는 사용자들의 권한 문제는 이를 이용한 IP 스푸핑 공격에는 그 탐지가 거의 불가능한 상황이다. 그러므로 새로운 원격지 접속에 대하여 업무의 연속성 보장과 인증 문제는 기업의 신뢰도와 직결되어 있다고 할 수 있다. 본 논문은 오늘날 다양해지는 공격으로부터 원격지에서 접속을 시도하는 정상적인 접속자의 권한 문제를 실시간으로 관련 데이터베이스에 적용하여 불법 접속에 대하여 능동적인 대응을 할 수 있도록 하였다. 아울러 정상적인 사용자와 비정상적인 사용자의 오탐율을 줄이면서 원격지 접속의 연속성과 신뢰성을 보장하고 있다.

A Design of Remote Access False-Positive Rate Improvement Model using Trace Route Information and Access Statistics Information

Hyun-Chul Baek*, Sang-Bok Kim**, Chang-Geun Kim***

ABSTRACT

Today the company adopts to use all business management at the network base such as internet, intranet and so on for the speed of business. Especially from a new remote access and user coming issue of the rights which an IP spoofing attack using a situation that is almost impossible to detect. Therefore, for a new remote access and authentication of business continuity issues are directly related to the company's reputation. Today's diverse, this paper attempts to connect from a remote access from the attack of the normal user rights issues related to real-time access to a database application for the illegal and decided to make an active response. In addition, normal and abnormal user false positive/negative rate of detection users to connect remotely, reducing the continuity and reliability are guaranteed.

Key Words : Trace router, False positive/negative rate, IP spoofing, Intrusion detection, Statics information

* 경상남도 진주의료원 전산실 (✉dosigas@lycos.co.kr)
** 경상대학교 컴퓨터과학과
*** 경상과학기술대학교 컴퓨터융합공학과
· 제1저자(First Author) : 백현철 · 교신저자(Correspondent Author) : 김창근
· 접수일(2011년 5월 10일), 수정일(1차 : 2011년 6월 30일), 게재확정일(2011년 7월 4일)

Ⅰ. 서 론

일반적인 기업내 네트워크는 안정성과 보안성을 위하여 다양한 보안 장비를 운영하고 있다. 아울러 원격지 사용자간에는 VPN(Virtual Private Network)]을[1] 구성하고 외부 공격에 대하여 방화벽, 침입탐지 시스템, 침입방지 시스템 등을 단독 또는 복합적으로 운영하고 있다[2][3]. 하지만 이러한 보안 시스템도 전혀 새로운 원격지에서의 인증된 사용자 접속에 대하여 능동적으로 대응하지 못하고 있다. 특히 IP 스푸핑 공격에 대하여 정상적인 사용자와 공격자를 분류할 수 있는 오탐율에 대하여 신뢰성 보장이 어렵다고 할 수 있다. 본 논문에서는 오탐율 개선 모델을 제안하여 기업내 직원이 어떠한 지역에 위치하더라도 신속한 인증을 한 다음 원격지 접속에 대하여 신뢰성과 가용성의 보장이 가능하도록 하였다. 아울러 IP스푸핑 공격에 대하여도 내부망에 대한 보호가 가능하도록 하였다. 본 논문의 구성은 Ⅱ장에서는 기존 네트워크 관련공격, 트레이스 라우트 정보, 통계자료를 이용한 정보 수집, Ⅲ장에서는 시스템 구현을 위한 알고리즘을 제안하였다. 그리고 Ⅳ장에서는 시뮬레이션 및 평가 그리고 그 결과를 타 시스템과의 비교 분석 하였으며, 마지막 Ⅴ장에서는 결론 및 향후 과제에 대하여 정리하였다.

Ⅱ. 관련연구

2.1 IP 스푸핑 공격

IP 스푸핑은 IP 자체의 보안 취약성을 악용하여 자신의 IP 주소를 인증 된 접속자로 위장하여 불법 접속을 시도하는 것을 말한다[4][5]. 그림 1은 신뢰관계에 있는 두 시스템 사이에서 인증을 받지 않은 자가 자신의 IP 주소를 신뢰관계에 있는 사용자의 IP 주소로 바꾸어 타겟 호스트를 속이고 접속을 시도하는 것을 나타내고 있다. 그 다음 rlogin, rsh 등을 이용하여 타겟 호스트를 무력화 시킨다. 즉 공격자가 마치 타겟 호스트가 신뢰하고 있는 접속자인 것 같이 위장하여 접속을 시도하는 침입 형태를 말한다.

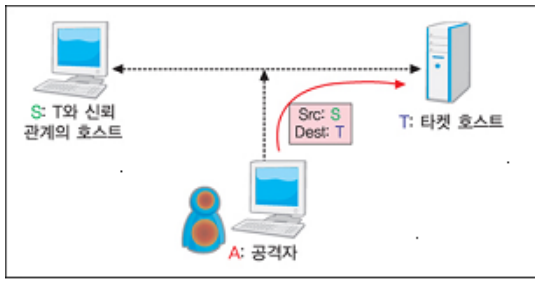

그림 1. IP 스푸핑의 예
Fig 1. Example of IP spoofing

2.2 트레이스 라우트 정보

트레이스 라우트란 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[6]. 트레이스 라우터를 통해 IP 주소나 URL로 목적지를 입력하면 각 구간마다 지나는 게이트웨이 컴퓨터의 이름이나 주소, 걸리는 시간 등이 표시되기 때문에 인터넷 경로상의 정보를 획득할 수가 있다[7].

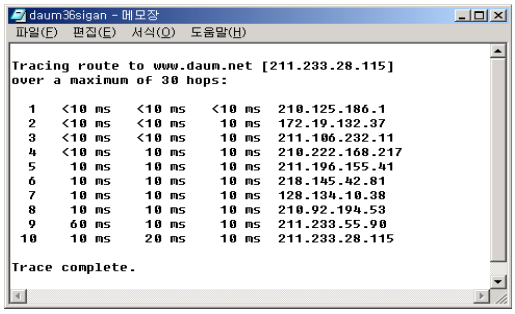

그림 2. 트레이스 라우트 정보
Fig 2. Trace route sampling

2.3 통계자료를 이용한 정보획득

통계적인 탐지 기술은 임계 탐지와 분석표 기반 시스템으로 분류를 한다. 임계 탐지는 시간 간격 상에서 특정한 사건 타입의 발생 빈도수를 세는 것이다. 분석표 기반 비정상 탐지는 개인 사용자의 지난 행동 또는 사용자의 그룹과 관련된 지난 행동을 특성화 하는데 초점을 맞춘다. 이 접근의 기초는 감사 기록의 분석이다.[8] 본 논문에서는 일정기간 동안 원격지 접속자들의 접속 행위를 분석하여 인증 데이터베이스로 활용하였다. 가장 간단한 통계학적인 테스트는 특정 기간 상에서 매개변수의 평균과 표준편차를 측정하는 것이다. 이것은 평균 행동과 변화성을 반영한다. 평균과 표준 편차는 폭 넓은 다양한 카운터, 타이머, 자원 측정에 적용될 수 있다.

III. 오탐율 개선 모델 설계

3.1 개선모델 설계

본 논문에서 제안하는 오탐율 개선 모델은 상호간 인증하는 시스템간의 트레이스 라우트 정보와 원격지 접속자들의 로그인 아이디, 1일, 그리고 일정기간의 접속 횟수와 접속 시간대의 정보를 통계적으로 데이터 베이스화 시킨 다음, 그 정보를 이용하여 실시간으로 원격지에서 접속을 시도하는 사용자들의 정보와 비교하여 차단여부를 결정할 수 있게 하였다.

그림 3은 트레이스 라우트 정보를 수집하는 과정을 보이고 있다.

PORT_VALUE는 원격지에서 서버 접속이 가능한 telnet이나 ftp를 체크할 수 있는 값을 나타내는 데이터 항목이다. IN_OUT은 해당 패킷이 내부에서 외부로 나가는 것이면 0, 외부에서 내부로 들어오는 것이면 1로 설정되는 값이다. 본 논문에서는 외부에서 내부로 접근하는 경우에만 탐지 모듈을 실행하도록 하였다. IP_Value1은 보안 시스템에 구축할 접근경로 정보 테이블의 항목으로 접근 권한을 가진 노드들의 출발지 IP 주소다. 접근 권한을 가진 노드들은 모두 등록시켜 놓아야 하므로 IP_VALUE는 접근 권한을 가진 사용자 수가 N이면 IP_VALUE의 항목수도 N이 된다. IP_VALUE의 부항목에는 경유하는 모든 라우터들의 수를 나타내는 Hop_Counter와, 라우터들의 IP 주소 정보를 나타내는 RIP_ADDR를 가진다. 전체 홉의 수에는 자신의 IP 주소 정보도 포함되어 있으므로 전체 홉의 수가 N이면 RIP_ADDR의 수도 N이 된다. 트레이스를 통하여 얻은 라우팅 정보 중 홉의 수와 경유하는 라우터들의 IP 주소는 자료 수집 과정에서 항상 일치하지 않고 삼 개월 정도 실험에서 한 번에서 두 번 정도로 홉의 수가 다르게 나타나는 경우가 있었다.

```
PORT_VALUE    Character (2)
IN_OUT        Character (1)
IP_Value_1    Character (20)
  .
  Hop_Counter_11    Character (2)
  RIP_ADDR_11_1     Character (20)
  RIP_ADDR_11_2     Character (20)
    .
  RIP_ADDR_11_n     Character (20)
 Hop_Counter_12     Character (2)
  RIP_ADDR_12_1     Character (20)
    .
  RIP_ADDR_12_n     Character (20)
    .
    .
IP_Value_n    Character (20)
 Hop_Counter_n1     Character (2)
  RIP_ADDR_n1_1     Character (20)
  RIP_ADDR_n1_2     Character (20)
    .
  RIP_ADDR_n1_n     Character (20)
 Hop_Counter_n2     Character (2)
  RIP_ADDR_n2_1     Character (20)
  RIP_ADDR_n2_2     Character (20)
    .
  RIP_ADDR_n2_n     Character (20)
```

그림 3. 트레이스 라우트 정보
Fig 3. Proposed trace-route information

그러므로 본 논문에서는 홉의 수를 Hop_Counter11과 Hop_Counter12 두 가지 경우로 구축했다. Hop_Counter를 한 가지만 정의를 하게 되면 접근 권

한을 가진 사용자의 인증을 위하여 원타임 패스워드 전송에 대한 오버헤드가 증가할 수 있다. 원타임 패스워드란 사용자의 ID와 패스워드를 인증 기반으로 하고 있는 UNIX 시스템에서의 패스워드 누출 문제와 최근 네트워크 감청을 통한 ID와 패스워드 유출 등으로 인한 불법 접속 시도 등 각종 위협에서 전산망을 안전하게 운용하기 위하여 적용하고 있는 전산망 원격 사용자 인증 기술이다[9]. 인증된 사용자들의 일상적인 원격지 접속 정보는 그림 4와 같이 접속자의 로그인 ID, 일일 로그인 시간과 특정기간의 로그인 정보의 평균치와 편차를 계산하여 이용하였다.

```
PORT_VALUE    Character (2)
IP_Value_1      Character (20)
LOGIN_NOR_ID       Character (10)
  L_IN_TIME_DAY
    L_IN_STR_AVG   HH/MM/SS
    L_IN_STR_VAR   HH/MM/SS
    L_IN_END_AVG   HH/MM/SS
    L_IN_END_VAR   HH/MM/SS
    L_IN_EX_AVG    HH/MM/SS
    L_IN_EX_VAR    HH/MM/SS

PORT_VALUE    Character (2)
IP_Value_1      Character (20)
L_IN_COUNT
  LOGIN_ID_CNT_DAY   Character (10)
  LOGIN_ID_CNT_TERM  Character (10)
```

그림 4. 로그인 정보
Fig. 4 Proposed login information

로그인 시간은 하루 업무시작, 마감 시간대, 그 외 시간대로 구분하여 정보를 수집하여 평균치와 편차로 통계 자료를 구성하였다. PORT_VALUE는 그림 3에서와 같이 원격지에서 서버 접속이 가능한 telnet이나 ftp를 체크할 수 있는 값을 나타내는 데이터 항목이다. 또 IP_Value1은 보안 시스템에 구축할 접근경로 정보 테이블의 항목으로 접근 권한을 가진 노드들의 출발지 IP 주소다. LOGIN_NOR_ID는 일상적인 접속을 시도하는 업무 시작시간의 평균 접속 시간대와 편차를 고려하여 각각 L_IN_STR_AVG, L_IN_STR_VAR 부터 L_IN_EX_AVG, L_IN_EX_VAR로 구성하였다. 그리고 일일 접속시간과 특정 기간의 접속 횟수는 LOGIN_ID_CNT_DAY, LOGIN_ID_CNT_TERM으로 구성하였다.

아울러 새로운 원격지 접속 정보 수집은 실시간으로 인증 데이터베이스 정보로 이용하기 위하여 별도로 L_IN_EX_AVG와 L_IN_EX_VAR을 이용하여 이들의 평균과 편차를 수집 한 다음 실시간으로 데이터베이스 정보로 이용한다.

3.2 인증정보를 이용한 불법 사용자 탐지과정

본 논문에서 구축하고자 하는 불법 사용자들에 대한 탐지과정은 다음과 같다. 불법 사용자는 보안시스템의 접근 정보인 로그인 아이디와 패스워드, 그리고 외부에서 내부망으로 접근 가능한 노드의 아이피를 알아낸 후 보안시스템으로 접근을 시도한다. 그 다음 원격 접속이 가능한 telnet이나 ftp 포트를 통하여 타겟 서버로 접근을 시도한다.

본 논문에서는 그림 3, 그림 4로부터 생성된 인증 데이터베이스를 이용하여 원격지 접속자의 접속 여부를 결정한다. 상호간 인증을 하고 있는 각 노드들은 그림 5와 같이 각각 인증 데이터베이스 정보를 공유하고 있다. 아울러 원격지 접속자들의 로그인 정보를 통계화하여 인증에 이용하고 있기 때문에 정상적인 사용자들을 차단하는 경우와, 공격자를 정상적인 사용자로 판정하는 오탐율을 크게 줄일 수 있다. 특히 정상적인 사용자가 인증 데이터베이스에 없는 전혀 새로운 지역에서 접속을 시도할 경우에도 통계화 시켜 구축 해 놓은 사용자 로그인 정보와 비교하여 일단 접속을 허용한다. 그 다음 휴대용 암호코드표를 이용하여 인증을 받아 연결에 대한 가용성을 높였다. 다음은 트레이스 정보와 원격지 접속 확률 정보를 이용한 탐지과정이다.

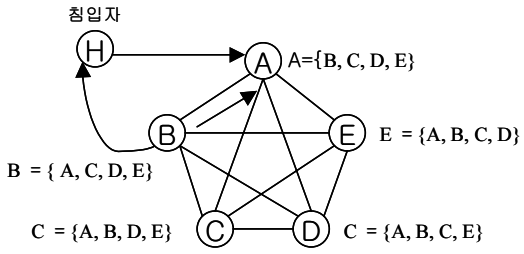

그림 5. 노드 상호간 구성 정보
Fig. 5 Trace information composition between nodes

그림 5의 침입자 H가 외부에서 노드 B의 정보를 이용하여, 노드 A로 IP 스푸핑을 시도 해 올 경우, 본 논문에서는 접근 권한을 가진 노드들의 트레이스 라우트 정보와 통계화 되어있는 로그인 정보를 각 노드들의 보안 시스템에 구축해 놓았기 때문에 침입자 H가 노드 A로 직접 접근을 시.도 하거나, 노드 B의 정보를 이용하여 IP 스푸핑을 시도해 올 때 모두 탐지를 한 다음 즉각적인 차단을 할 수 있다.

Ⅳ. 시뮬레이션 및 평가

4.1 실험

실험 환경은 그림 6과 같이 실험을 위한 네트워크를 구성하고, Windows XP 운영체제에서 Visual C++6.0을 이용하였으며, 네트워크는 10Mbps LAN상의 동일한 네트워크에서 시뮬레이션 하였다. 실험을 위한 자료는 일정기간 내부 노드에 트레이스 라우트 정보와 로그인 정보 자료를 구축하고, 외부노드에서 내부 노드로 접근을 시도하는 방식을 택하였다.

실험 과정은 불법 사용자의 접근을 외부 노드에서 내부 노드 쪽으로 인증 데이터베이스에 없는 IP 주소와 접근 정보를 가지고 내부 노드로 접근하는 것으로 가정했다. 그리고 내부에 구축되어 있는 인증 데이터베이스의 정보인 트레이스 라우트 정보와 로그인 정보를 가지고 접근을 시도하면 정상 사용자로 가정하였다. 다음은 전혀 새로운 장소에서 원격지 접속을 시도하는 정상적인 접속자일 경우를 가정하였다. 이 경우는 첫 번째 인증 데이터베이스에 없는 트레이스 라우트 정보에도 없고, 로그인 정보와 일치성을 비교하여 둘 다 일치성이 없는 경우 차단을 하고 암호화된 원-타임 패스워드를 발생시켜 재접속을 요구한다.

그림 6. 실험을 위한 네트워크 구조
Fig 6. Network architecture for experiment

하지만 본 논문에서는 트레이스 라우트 정보가 일치하지 않지만 로그인 정보가 일치하면 일단 접속을 허용하고, 휴대용 암호코드표의 추가정보를 이용하여 접속을 가능하게 하여 시스템 가용성을 높일 수 있다. 이상과 같이 제안 모델과 기존의 방화벽 시스템, 침입탐지 시스템과의 비교 결과는 표 1에서 보이고 있다.

표1. 제안방식 비교 테이블
Table 1. Proposed method vs. Intrusion detection system vs. Firewall

형태 / 요소	침입탐지시스템	방화벽	제안방식
데이터 수집	시스템이벤트 네트워크 패킷	네트워크 패킷, 프로토콜	접근경로/로그인 정보수집
데이터 가공	데이터축약 데이터가공	없음(대부분 설정 Rule 로 결정)	접근경로정보와 로그인정보가공
오탐율	다양한 패턴분석으로 인한 오버헤드, False Negative/Positive 오류 발생	설정 Rule비교로 차단여부 결정	로그인정보, 암호코드표추가, FalseNegative/Positive 오류 감소
접근패턴 /로그인 정보 유출시 기능	False Negative발생으로 탐지 불가능	차단기능상실	접근경로/로그인 정보, 암호코드표 이용으로 탐지/차단
새로운 원격지 접속 서비스 지속성	정상 사용자인 경우도 서비스 차단 발생	설정 Rule과 비교후 침입서비스 차단	접근 경로/로그인 정보, 암호코드표 이용으로 서비스 가능

Ⅴ. 결론 및 향후 과제

본 논문의 오탐율 개선 모델은 트레이스 라우트 정보와 인가된 원격 접속자들의 로그인 정보를 통계화하여 효과적인 그 개선 모델을 제시한 것이다. 그리고 본 논문에서 제안하는 오탐율 개선 모델은 하드웨어적인 비용의 추가부담이 거의 없다고 할 수 있다. 아울러 오탐율의 개선으로 원격지 접속의 연속성과 신뢰성의 보장으로 인한 업무의 신뢰도와 시스템의 가용성 또한 증대 시킬 수 있고, 기업의 이미지 상승효과도 있다. 향후 고려해야할 부분은 모바일 접속 상황에서의 불법 접속 가능성에 대한 연구가 병행되어야 할 것이다.

참고문헌

[1] Farkhod Alisherov, Nayoun Kim, Eun-suk Cho, Seok-soo Kim, "Penetration testing a VPN," *한국정보기술학회 2009년도 Green IT 융합기술 워크숍 및 하계 종합 학술 대회 논문집* 2009.6, pp. 903~905(3pages)

[2] 양환석, "침입탐지시스템 성능향상을 위한 룰 적용에 관한 연구," *한국차세대컴퓨팅학회 논문지*, 제 5 권, 제 3 호, 2009.

[3] 손형서, 김현성, 부기동, "암호화 기법을 적용한 침입 탐지 시스템의 보호 기법," *정보보호학회 논문지*, 제 14 권, 제 6 호, 2004.

[4] 김봉한, 이재광, 백승현, 오형근, 박응기, "침입 탐지 도구에서 능동 대응 정책 생성 방안," *한국콘텐츠학회논문지*, 제 6 권, 제 1 호, 2006.

[5] 정영식, "침입 탐지 및 대응 연구 동향" *보안공학연구 논문지*, 제 3 권, 제 4 호, 2006.

[6] 정종민 ,이지율 ,이구연, "역추적 에이전트를 이용한 역추적 시스템 설계 및 구현," *강원대학교 산업기술연구소*, 제 22 권, 제 B 호, 2002.

[7] 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, 2009.6, pp.157-163.

[8] 이수진, 정병천, 김희열, 이윤호, 윤현수, 김도환, 이은영, 박응기, "연관성을 이용한 침입탐지 정보 분석 시스템의 설계 및 구현," *정보과학회 논문지*, 제 31 권, 제 5 호, 2004.

[9] 이용호, 박희운, 이임영, "새로운 일회용 패스워드 방식 제안," *한국정보처리학회 춘계학술발표 논문집*, 제 8 권, 제 1 호, 2001.

감사의 글

본 논문은 2010년도 경남과학기술대학교 기성회 연구비 지원으로 수행되었음.

저자소개

백현철(Hyun-chul Baek)

2003년 경상대학교 (공학박사)
2007년 전국지방의료원 전산기술위원장
현재 경상남도 진주의료원 전산실장
※ 관심분야 : 네트워크, 네트워크보안

김상복(Sang-Bok Kim)

1989년 중앙대학교 (공학박사)
2007. 12 ~ 2010. 8 경상대학교 교육정보전산원장
현재 경상대학교 컴퓨터과학과 교수, 경상대학교 컴퓨터정보통신연구소원
※ 관심분야 : 컴퓨터네트워크, 컴퓨터구조

김창근(Sang-Bok Kim)

1999년 경남대학교 (공학박사)

현재 경남과학기술대학교 컴퓨터융합공학과 교수
※ 관심분야 : 데이터통신 및 이동통신, 홈네트워킹, 유비쿼터스 네트워킹