논문 14-39C-08-13
The Journal of Korea Information and Communications Society '14-08 Vol.39C No.08
http://dx.doi.org/10.7840/kics.2014.39C.8.716

# 데이터베이스에서 지정된 IP 주소 접근 금지를 위한 기능 설계

장 승 주◆°, 김 성 진*

# Design of the Specific IP Access Deny for the Database

Seung-Ju Jang◆°, Sung-Jin Kim*

요 약

본 논문은 Oracle 데이터베이스의 환경과 C 프로그램 환경에서 원격으로 IP 주소를 사용하여 해킹 등의 보안 취약점을 공격하는 것을 예방하고, 문제점을 해결한다. 공격자가 원격으로 IP 주소를 사용하여 데이터베이스 로그인을 시도하여 데이터를 해킹 하는 경우가 많다. 최근에는 해외의 IP 주소를 사용하여 로그인 하는 경우도 자주 발생하고 있으며, 노출된 데이터베이스 계정을 이용하여 로그인을 시도하고 있어, 데이터베이스의 데이터 노출 위협이 높아지고 있다. 본 논문은 Oracle 데이터베이스의 특정 IP 차단 모듈을 개발하여 특정 IP를 차단 혹은 제어함으로써 악의적인 사용자가 데이터베이스에 접근할 수 없도록 한다.

**Key Words :** Oracle, Database, DB Vulnerability, IP blocking, DB Listener

ABSTRACT

This paper proposes how to prevent of vulnerability from IP address attack of Oracle DB by C program environments. An attacker may try to login DB by connectng remote IP address. Recently an attacker use foreign IP address and try to connect to DB using known DB account. Therefore, DB data is frequently disclosed. I propose a new idea that develops specific IP address blocking module in C program in the Oracle DB. By this module, we can use the Oracle DB safely.

## Ⅰ. 서 론

본 논문은 Oracle 데이터베이스의 보안 취약점을 점검함으로써 허락받지 못한 사용자의 접근을 제한하도록 한다. 보안 점검을 통하여 발견된 취약점은 관리자에게 경고 메시지 보내고 취약점을 수정할 수 있도록 한다. 이와같이 취약점을 예방하고, 문제를 해결함으로써 사용자들의 정보를 안전하게 보호 할 수 있도록 설계하여 프로그램으로 구현한다.

Oracle은 원격에서 데이터베이스 서버로의 접속을 제한하지 않으면 치명적인 허점이 될 수 있다. 더 나아가 특정 IP를 제어하지 않으면 악의적인 사용자가 원격으로 IP 주소를 사용하여 데이터베이스 로그인을 시도한 후 데이터베이스를 해킹하는 경우가 많다. Oracle Listener 운영 시 중요한 정보들이 노출될 수 있고, 이러한 노출 정보가 많으면 많을수록 데이터베이스가 공격 당 할 가능성이 더 높아진다.

Oracle에서 임의의 사용자에 의한 원격 접속을 차단하기 위해 Listener의 IP 접근 제한을 설정할 수 있다. 특정 클라이언트에서의 접근만 가능하도록 접근

※ 이 논문은 2014학년도 동의대학교 교내연구비에 의해 연구되었음(2014AA005).
◆° First and Corresponding Author : Dongeui University Department of Computer Engineering, sjjang@deu.ac.kr, 정회원
* Dongeui University Department of Computer Engineering, makeitso@deu.ac.kr
논문번호 : KICS2014-05-189, Received May 20, 2014; Revised August 1, 2014; Accepted August 1, 2014

가능 IP를 설정하여 불필요한 외부의 사용자가 접근하는 것을 차단할 수 있다. 또한, 특정 IP에 대한 접근 제어도 가능하다. 환경 설정 파일에서 접근 가능한 IP 대역과 접근 불가능한 IP대역을 설정하여 네트워크 접근통제를 할 수 있다. Oracle의 Listener 설정 파일인 sqlnet.ora 내의 파라미터를 설정하면 원격에서 Oracle 특정 IP 차단 기능을 사용할 수 있다.[1]

본 논문에서 개발한 Oracle IP Block 프로그램에서는 특정 IP에 대해 차단 기능이 설정되어 있는지 확인하고, 만약 설정되어 있지 않다면 보안 취약점이 있는 것으로 판단을 한다. Oracle의 특정 IP를 차단 혹은 제어하게 되면 불필요한 IP 주소나 공개된 악의적인 IP 사용자들을 차단, 제어함으로서 보안 취약점을 해결할 수 있다.

본 논문의 구성은 2장에서 기술 개발의 필요성 및 중요성을 언급한다. 3장에서는 본 논문에서 제시하는 Oracle 특정 IP 차단 프로그램 설계 목표를 설명한다. 4장은 Oracle 특정 IP 차단 프로그램 구현을 설명한다. 5장에서는 결론을 내린다.

## Ⅱ. 관련 연구

보안 취약점 (Vulnerability)은 좁은 의미로 컴퓨터의 하드웨어 또는 소프트웨어의 결함이나 체계 설계상의 허점으로 인해 사용자 (특히, 악의를 가진 공격자)에게 허용된 권한 이상의 동작이나 허용된 범위 이상의 정보 열람을 가능하게 하는 약점이다. 넓은 의미로는 좁은 의미에 더하여 사용자 및 관리자의 부주의나 사회공학 기법에 의한 약점을 포함한 정보체계의 모든 정보 보안상의 위험성을 말한다. 악의를 가진 공격자는 이러한 약점을 이용하여 공격 대상 컴퓨터 또는 정보화 기기에서 공격자가 의도한 동작을 수행하게 하거나 특정한 정보를 탈취한다. 보안 취약성 또는 취약성으로 부르기도 한다[1,2,6-9].

DB 침해 사고는 외부의 해커, 인가된 내부 사용자, 인가되지 않은 내부 사용자 등 모든 범위에서 발생할 수 있다. DB는 정보시스템의 가장 깊은 곳에서 운영되지만 웹 애플리케이션(Web Application), 내부망(internal Network), 파트너 연계 네트워크 등 수많은 접근성의 존재로 인해 데이터 유출 위험이나 서비스 중지의 위험이 상시적으로 존재한다.

DB 취약점은 해커들에 의해 항상 공개가 된다. 이렇게 공개된 DB 취약점들을 통해 DB는 쉽게 공개 대상으로 주목된다. DB 취약점 분석은 DB에 내재된 취약점들과 DB 운영에 있어서 고려되어야 할 항목들을 다각도에서 구체적으로 점검함으로써 보안 관리자 및 DBA에게 시스템에 내재된 안전 취약점(Security Hole)을 제거하게 하여 DB의 보안 수준을 향상시키게 한다. DB 취약점 분석은 점검대상 네트워크 범위에 존재하는 정보자산을 파악하는 정보 수집(Information Gathering), DB 보안을 검증할 수 있는 모의해킹(Penetration Test), 내부 보안감시(Security Auditing) 등의 과정을 통해 다양한 DB 취약점들을 도출하여 정보 자산의 파악과 보안성의 검토, 검출된 취약점 제거를 위한 Fix Scripts 및 개선안 제시, 레포팅 등을 주요 항목으로 한다[3-5,10-13]. 아래의 Fig. 1은 데이터베이스의 취약점 분석 절차에 대한 그림이다.

취약점 공격 또는 익스플로잇(exploit)이란 컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 절차나 일련의 명령, 스크립트, 프로그램 또는 특정한 데이터 조작을 말하며, 이러한 것들을 사용한 공격 행위를 이르기도 한다. 취약점 공격은 주로 공격 대상 컴퓨터의 제어 권한 획득이나 서비스 거부 공격 등을 목적으로 한다.

취약점 공격이 만들어지는 시점은 취약점이 얼마나 널리 알려졌는지와 관계없지만, 취약점 공격이 널리 공개되는 시점은 보통 해당 취약점이 널리 알려진 후이다. 보통은 이러한 시점에 이르기 전에 해당 취약점을 보완한 업데이트가 공개되므로 항상 최신의 업데이트를 적용하여 취약점을 보완하거나 최신 버전의 바이러스 검사 등을 이용하면 위협에 대한 노출을 줄일 수 있다. 하지만 이외의 취약점 공격의 대책은 미흡하여 여전히 보안의 위협에 노출이 될 가능성이 크다. 본 논문에서 개발한 프로그램으로는 특정 IP의 보안 취약점이 존재 하는지 하지 않는지를 판단을 하여 존재 한다면 경고 메시지를 보내 주고 특정 IP 차단

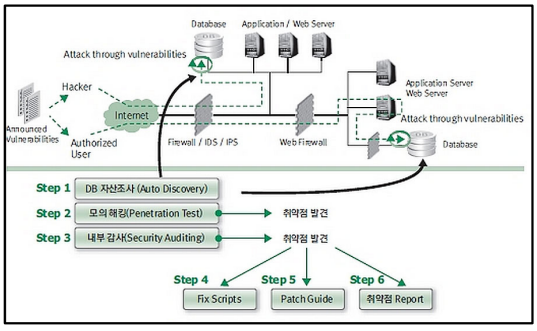


그림 1. DB 취약점 분석 절차
Fig. 1. DB Vulnerability Analysis Procedures

기능을 수행할 수 있도록 한다. 보안 취약점 체크를 함으로써 위험성에 대한 노출을 더욱 줄일 수 있다[2-5].

## Ⅲ. Oracle 특정 IP 차단 프로그램 설계

본 논문은 Oracle 데이터베이스의 특정 IP를 차단하여 공개된 악의적인 사용자의 IP나 공개된 IP를 차단하는 프로그램을 설계한다. 본 논문에서 제시하는 Oracle IP Block 프로그램은 Oracle 데이터베이스의 리스너 설정 및 C언어로 프로그램을 작성하여 설계한다.

Fig. 2는 Oracle 데이터베이스의 시스템 서비스 구조이다. 데이터베이스가 작동되는 단계별 과정을 보면 각 Oracle 데이터베이스는 Oracle 인스턴스와 연관된다. 데이터베이스가 시작되면 SGA 공유 메모리 영역을 할당하고 여러 가지 백그라운드 프로세스를 시작하게 된다. 다음으로 인스턴스 시작 후 소프트웨어가 특정 데이터베이스와 인스턴스를 연관시킨다. 이를 디스크 마운트라고 한다.

리스너(Listener)는 Oracle 데이터베이스에 원격으로 접속하기 위해서 필요한 프로세스이다. 원격의 클라이언트에서 접속을 위해서 반드시 필요한 것이며 리스너 프로세스는 서버 측 백그라운드 프로세스(Background Process)로서 클라이언트의 접속을 리스닝하기 위해 1521 포트를 기본적으로 사용하고 있다. Oracle Instance가 시작되면 PMON(Process MONitor)이 리스너 프로세스에게 자신이 관리하는 Database 명을 등록하고 리스너 프로세스를 기동하기 위해서는 c:>lsnrctl start 라고 한다. 원격의 클라이언트에서 오라클 서버로 접속을 요구할 때 클라이언트가 오라클 서버의 1521포트에 접속을 요청하며 서버의 리스너 프로세스가 클라이언트에서 요청하는 오라클 서버가 자신이 관리하는 인스턴스에 있으면 서버 프로세스에게 요청을 넘긴다. 이때 이 사용자에 대해 새로운 네트워크 번호(포트)가 할당되는데 이후부터 클라이언트는 이 포트를 통해 Oracle Server Process와 직접 통신을 하게 된다. 클라이언트에는 파일에 접속할 Oracle Server의 이름, IP 주소 등을 정의하는 tnsnames.ora 파일이 있고 실제 Oracle Server의 특정 IP만 제한하거나 허용하기 위해서는 $ORACLE_HOME/network/admin 아래의 sqlnet.ora 파일에 다음 Fig. 3과 같이 설정 한다[4].

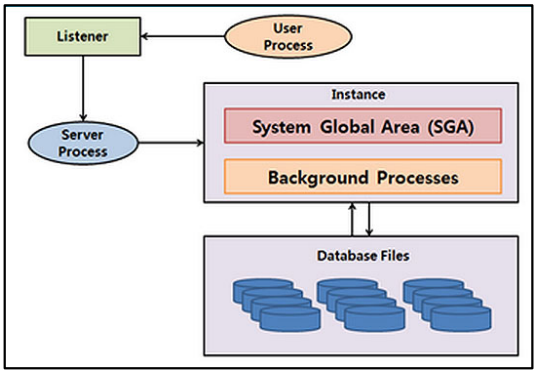


그림 2. Oracle 데이터베이스 시스템 서비스 구조
Fig 2. Oracle Database System Service Structure

Fig. 3은 접근 통제를 할 IP 주소 및 네트워크 대역을 추가해서 설정할 수 있다. TCP.VALIDNODE_CHECKING를 YES로 설정한 후 접속을 차단할 IP 주소 또는 호스트 네임을 TCP.EXCLUDED_NODES에 넣어주면 된다. 만약 주석처리(#)가 되어 있다면 주석을 풀어야만 적용이 된다. sqlnet.ora 파일을 수정한 후에는 Listener를 재 시작해야 해당 설정이 적용된다. 본 논문에서는 이와같이 Oracle 데이터베이스의 특정 IP 차단 기능을 C 프로그램을 이용하여 사용자들에게 보다 편리하고 쉽게 차단 설정을 할 수 있도록 설계하였다.

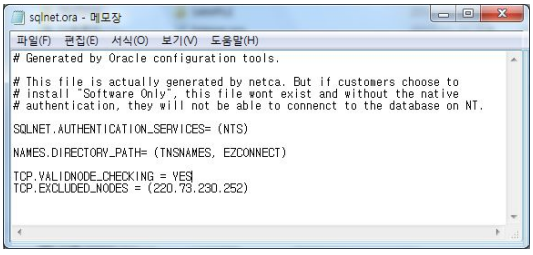


그림 3. sqlnet.ora
Fig. 3. sqlnet.ora

## Ⅳ. Oracle 특정 IP 차단 프로그램 구현 및 실험

본 논문에서는 Oracle 데이터베이스의 특정 IP 차단 기능을Visual Studio 2008 환경의 C 프로그램을 이용하여 개발하였다. 먼저 Oracle 데이터베이스가 설치되어 있는지를 체크하고 Oracle sqlnet의 경로를 나타내어 주며 Oracle 데이터베이스의 sqlnet.ora 파일의 내용을 보여준다. 특정 IP를 차단하는 기능은 TCP.VALIDNODE_CHECKING = YES, TCP.EXCLUDED_NODES = ( IP ) 일 경우 IP 주소를 차단할 수 있다. 만약 이 부분이 #(주석 처리)가 되어 있거나 YES가 아닌 NO일 경우 특정 IP 주소 차단 설정 기능이 되어 있지 않는 것으로 보안 취약점이 있는 것으로

판단한다.

Fig 4 는 개발된 프로그램을 실행한 모습이다. 현재 TCP.VALIDNODE_CHECKING = NO 상태이고, #(주석처리)가 되어 있는 상태이므로 보안 취약점이 있는 상태이다. 그래서 수정을 권하는 경고 메시지를 보내어 주고 사용자는 (1:YES 2:NO) 중 선택을 하게 된다. 현재 (2:NO)를 선택했기 때문에 '외부 접속 IP에 대한 차단 기능을 설정되어 있지 않습니다. 보안 취약점이 있습니다. 시스템을 점검하기 바랍니다.' 라는 경고 메시지를 보내준다.

Fig. 5는 Fig. 4와 TCP.VALIDNODE_CHECKING, TCP.EXCLUDED_NODES 의 상태를 다르게 하여 프로그램을 실행한 모습이다. 현재 TCP.VALIDNODE_CHECKING = NO 상태를 YES로 변경하고 TCP.EXCLUDED_NODES = ( IP ) 설정이 되어 있지만 #(주석처리)가 하나라도 되어 있기 때문에 특정 IP 차단 기능이 설정되어 있지 않은 것으로 보안 취약점이 있는 것으로 판단하여 '외부 접속 IP에 대해서 차단 기능이 설정되어 있지 않습니다. 보안 취약점이 있습니다. 시스템을 점검하기 바랍니다.' 라는 경고 메시지를 보내준다.

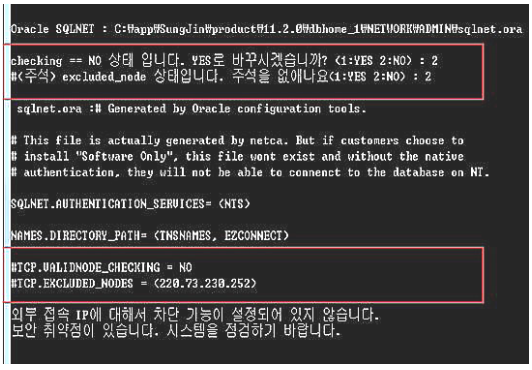


그림 4. # TCP.VALIDNODE_CHECKING = NO # TCP.EXCLUDED_NODES = ( IP )
Fig. 4. # TCP.VALIDNODE_CHECKING = NO # TCP.EXCLUDED_NODES = ( IP )

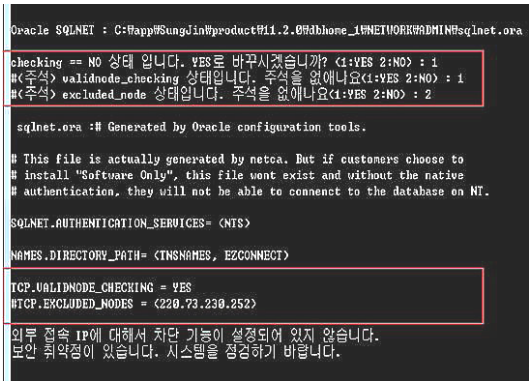


그림 5. TCP.VALIDNODE_CHECKING = YES # TCP.EXCLUDED_NODES = ( IP )
Fig. 5. TCP.VALIDNODE_CHECKING = YES # TCP.EXCLUDED_NODES = ( IP )

Fig. 6 은 TCP.VALIDNODE_CHECKING = NO 상태를 YES로 변경하고 TCP.EXCLUDED_NODES = ( IP ) 설정이 되어 있고 #(주석)을 풀었기 때문에 특정 IP 차단 기능이 설정되는 것으로 보안취약점이 없는 것으로 판단한다. 위와 같은 다양한 실험 결과, 본 논문에서 제안하는 특정 IP 주소에 대한 차단 기능이 오라클 DB에서 정상적으로 동작됨을 확인할 수 있었다.

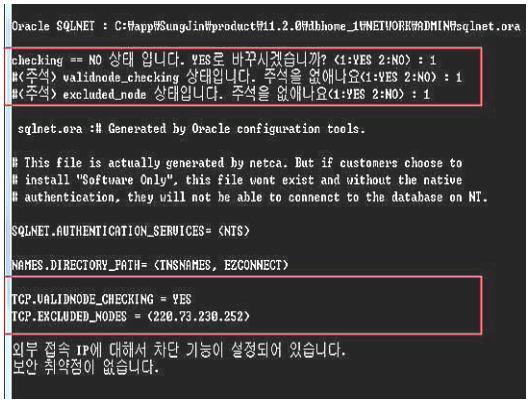


그림 6. TCP.VALIDNODE_CHECKING = YES TCP.EXCLUDED_NODES = ( IP )
Fig. 6. TCP.VALIDNODE_CHECKING = YES TCP.EXCLUDED_NODES = ( IP )

## V. 결 론

데이터베이스 보안은 사용자로부터 조직 또는 개인의 정보 유출에 대한 방어를 목적으로 한다. 데이터베이스 보안 취약점들은 사용자의 실수나 공개된 취약점 등으로부터 기인하게 된다. 악의적인 사용자의 권한 접근으로 인해 비정상적인 접근행위를 하게 된다면 그 위험요소는 사용자들에게 큰 피해를 입힐 것이다. 오늘날의 정보자산은 무형의 자산뿐만 아니라 실질적인 재화를 의미하며, 이러한 가치의 증대로 인하여 주요 기업 정보가 집중되는 데이터베이스에 대한 위협들이 나날이 증가하고 있다.

본 논문에서 제안하는 DB(Database) 보안 취약점 점검 기능은 Oracle 데이터베이스의 보안 취약점 점검을 통하여 허락되지 않은 사용자의 접근을 제한하

도록 한다. 보안 점검을 통하여 발견된 취약점은 경고 메시지를 사용자에게 보내주게 된다. 이러한 기능은 취약점을 예방함으로써 사용자들의 정보를 안전하게 보호 할 수 있도록 설계하여 프로그램으로 구현하였다. 보안 취약점 점검 기능으로 구현된 프로그램을 구동시키고 정상적으로 동작하는지의 여부를 실험하여 사용자들의 정보를 보다 안전하게 보호할 수 있다. 본 논문에서 개발한 프로그램을 이용하여 실험을 하였고, 실험 결과 정상적으로 특정 IP 주소가 차단됨을 확인할 수 있었다.

## References


[1] J. S. Kim, *DB security for the protection of personal information(2006)*, Retrieved Dec., 10, 2013, from http://blog.naver.com/mybrainz/150007657976

[2] *Wikipedia vulnerability(2012)*, Retrieved Dec. 12, 2013, from http://ko.wikipedia.org/

[3] *DB Vulnerability Analysis Summary*, Retrieved Dec. 20, 2013, from www.DBGuide.net

[4] *Listener(2009)*, Retrieved Dec., 2, 2013, from http://www.netbuysell.co.kr/global_asp/board/board_view.asp?Codeno=5&K_no=359&Pgtype=A

[5] S. H. Lee, Y. J. Maeng, D. H. Nyang, and K. H. Lee, "Possibility of disclosure of user information in internet explorer," *J. KICS*, vol. 38B, no. 12, pp. 937-943, 2013.

[6] J. H. Lee, J. S. Park, S. W. Jung, and S. Jung, "The authentication and key management method based on PUF for secure USB," *J. KICS*, vol. 38B, no. 12, pp. 944-953, 2013.

[7] W. S. Seo and M. S. Jun "The management and security plans of a separated virtualization infringement type learning database using VM (virtual machine)," *J. KICS*, vol. 36, no. 8, pp. 947-953, 2011.

[8] P.-H. Jo, J.-I. Lim, and H.-K. Kim "A study on improvement of security vulnerabilities in intelligent transport system," *J. The Korea Inst. Inf. Security & Cryptology(JKIISC)*, vol. 23, no. 3, pp. 531-543, 2013.

[9] D.-J. Kim and S.-J. Cho "An analysis of domestic and foreign security vulnerability management systems based on a national vulnerability database," *Internet Inf. Security*, vol. 1, no. 2, pp. 130- 147, 2010.

[10] I.-Y. Mun and S.-M. Oh "Vulnerability analyzers for the mobile application the design and implementation," *J. Korea Multimedia Soc.*, vol. 14, no. 10, pp. 1335-1347, Oct. 2011.

[11] S.-M. Yang and J. S. Park "An efficient access control mechanism for secure surveillance systems," *J. KICS*, vol. 39B, no. 4, pp. 228-233, 2014.

[12] J.-S. Park, M.-H. Park, and S.-H. Jung "A whitelist-based scheme for detecting and preventing unauthorized AP access using mobile device," *J. KICS*, vol. 38B, no. 8, pp. 632-640, 2013.

[13] H.-U. Yoo, J.-H. Yun, and T.-S. Shon "Whitelist-based anomaly detection for industrial control system security," *J. KICS*, vol. 38B, no. 8, pp. 641-653, 2013.

[14] Y.-H. Lee, J. H. Kang, and S. J. Lee "A specification-based intrusion detection mechanism for LEACH protocol," *J. KICS*, vol. 37B, no. 2, pp. 138-147, 2012.



**장 승 주** (Seung-Ju Jang)

1985년 : 부산대학교 계산통계학(전산학) 학사

1991년 : 부산대학교 계산통계학(전산학) 석사

1996년 : 부산대학교 컴퓨터공학 박사

1987년~1996년 : 한국전자통신연구원(ETRI) 시스템 SW연구실

1993년~1996년 : 부산대학교 시간강사

2000년~2002년 : Univ. of Missouri at Kansas City, visiting professor

1996년~현재 : 동의대학교 컴퓨터공학과 교수

<관심분야> 운영체제, 임베디드 운영체제, 분산시스템, 시스템 보안, 스마트 폰 시스템 운영체제

**김 성 진** (Sung-Jin Kim)

2006년 : 동의대학교 컴퓨터공학 학사 입학
2013년 : 동의대학교 컴퓨터공학 학사 졸업
2013년 : 동의대학교 컴퓨터공학 석사 입학
<관심분야> 운영체제, 임베디드 운영체제, 데이터베이스 보안, 네트워크 보안