韓國컴퓨터情報學會 論文誌
第14卷 第12號, 2009. 12.

2009-14-12-3-8

DBMS WAS 우회접속의 쿼리정보 역추적 연구

백 종 일*, 박 대 우**

A Study on Traceback by WAS Bypass Access Query Information of DataBase

Jong-Il Baek*, Dea-Woo Park**

요 약

초고속 인터넷의 웹 서비스를 사용하여 WAS를 통한 DBMS 접근이 늘어나고 있다. 불특정 다수에 의한 DBMS에 대한 3-Tier와 우회접속에 대한 접근 및 권한제어를 위해서는 DB보안 기술의 적용이 필요하다. WAS를 통해 DBMS에 우회접속을 하면 DBMS는 우회접속 사용자의 IP정보를 저장하지 못하고, 직전 시스템에 접속한 사용자인 WAS의 정보를 저장하게 된다. 본 논문에서는 WAS를 통해 DBMS에 우회접속하는 쿼리정보를 역추적하여 보안감사기록과 포렌식자료를 연구한다. 통신 경로에서 MetaDB를 구축해 웹을 통해 login한 사용자에 대한 세션과 쿼리 정보를 저장하고, DBMS에도 로그 되는 쿼리 정보를 저장해서 time stamp 쿼리를 비교 매핑 하여 실제 사용자를 식별한다. 보안 신뢰성의 향상 방법으로, log을 받아 Pattern 분석 후에 Rule을 만들어 적용하고, Module을 개발해 정보의 수집 및 압축을 통해 데이터 저장소에 보관한다. 보관된 정보는 지능형 DB보안 클라이언트를 이용한 분석과 정책 기반 관리 모듈의 통제를 통해 역추적의 오탐률을 최소화할 수 있게 한다.

Abstract

DBMS access that used high speed internet web service through WAS is increasing. Need application of DB security technology for 3-Tier about DBMS by unspecified majority and access about roundabout way connection and competence control. If do roundabout way connection to DBMS through WAS, DBMS server stores WAS's information that is user who do not store roundabout way connection user's IP information, and connects to verge system. To DBMS in this investigation roundabout way connection through WAS do curie information that know chasing station security thanks recording and Forensic data study. Store session about user and query information that do login through web constructing MetaDB in communication route, and to DBMS server log storing done query information time stamp query because do comparison mapping actuality user discriminate. Apply making Rule after Pattern analysis receiving log by elevation method of security authoritativeness, and develop Module and keep in the data storing place

• 제1저자 : 백종일 교신저자 : 박대우
• 투고일 : 2009. 09. 09, 심사일 : 2009. 09. 30, 게재확정일 : 2009. 12. 26.
* 호서대학교 벤처전문대학원 IT응용기술학과 ** 호서대학교 벤처전문대학원 교수

through collection and compression of information. Kept information can minimize false positives of station chase through control of analysis and policy base administration module that utilize intelligence style DBMS security client.

▸ Keyword : DB보안(DB Security), WAS(Web Application Server), 우회공격(Bypass attack), 역추적기술(Trace Back), 접근제어(Access Control), 쿼리(Query)

Ⅰ. 서 론

인터넷사용에서 해킹에 의한 개인정보 유출사고는, 침입시도의 횟수뿐만 아니라, 정보가 유출된 사건으로 인한 개인정보에 대한 중대한 침해사고의 문제로 인식된다. 개인정보보호에 대한 DB(DataBase)보안의 중요성이 강조 되면서 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령〔전부개정 2008.2.29 대통령령 제20668호〕 제15조(개인정보의 보호조치) ①에서는 개인정보에 대한 불법적인 접근을 차단하기 위한 접근통제장치의 설치·운영 및 접속기록의 위조·변조 방지를 위한 조치 등을 다루고 있다〔2〕.

그림 1의 2008년 KISA 인터넷 침해사고의 동향을 보면 해킹으로 인한 정보침해가 심각하다. 위 분석 자료에 의하면 스팸공격에 대한 방지 및 예방기술이 발전하면서 스팸릴레이 공격은 현격히 줄어든 반면, 해킹공격은 아직도 꾸준한 추세이다〔1〕.

구분	2008년 총계	2009년												2009년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
웜·바이러스	8,469	460	641	695	925	941	837							4,499
해킹신고처리	15,940	1,579	1,119	1,285	1,582	1,863	2,319							9,747
- 스캠릴레이	6,490	617	495	599	764	1,134	1,290							4,899
- 피싱 경유지	1,163	65	72	86	51	88	100							462
- 단순침입시도	3,175	194	230	219	162	210	282							1,297
- 기타해킹	2,908	277	225	291	299	238	261							1,591
- 홈페이지변조	2,204	426	97	90	306	193	386							1,498
악성 봇(Bot)	8,1%	1,4%	2,0%	1,6%	1,6%	1,0%	0,9%							1,3%

그림 1. 인터넷 침해사고 통계
Fig 1. Internet infringement accident statistics

개인정보보호를 위해 DB서버에 접근하는 사용자들의 접근 및 권한을 제어하는 DB보안 솔루션들은 기본적으로 보안기능을 보유하고 있다. 그러나 분산 시스템의 증가와 인터넷의 확산으로 인하여 클라이언트/서버 환경에서 웹 환경으로 전환되면서, WAS(Web Application Server)를 통한 DBMS(Data Base Management System) 접근이 늘어나고 있어 잠재적인 공격의 위협으로부터 개인정보를 저장하고 있는 DBMS 시스템을 보호하기 위한 보안 대책이 필요하다.

기존의 DBMS 보안 솔루션들은 DBMS에 접근하는 내부자의 작업내역 확인을 목적으로 개발한 Sniffing 방식과 사용자 접근 및 권한통제를 Loss 없이 제어하기 위한 Gateway 방식이 대부분이다〔5〕.

그러나 기존 방식은 WAS를 통해 비정상적으로 DBMS에 접근하는 우회접속자들에 대한 정확한 로깅이 불가능 하다는 문제점이 있다. 또한 DBMS 서버와 WAS서버 사이에 실제 사용자를 식별하는 방법은 기술적으로 한계에 봉착되어 있다. 서로 다른 관리시스템을 통해 물리적으로 감사기록을 분석하는 방법, 반복되는 인증을 통한 로깅 외에는 효과적인 방법이 없어 가용성을 고려한 효율적인 개선안이 시급하다〔7〕.

본 논문에서는 중요 DBMS를 위한 WAS 우회접속 공격자에 대해 지능형 DBMS 보안 관리시스템을 통해 다차원 분석 기능 및 DBMS 접근 기록 검색 기능을 제공하여, 불법침입에 대한 능동적인 접근통제와 지능형 DBMS 보안 클라이언트를 이용한 분석으로 정책 기반 관리 모듈의 통제를 통해, 사후 감시 추적의 오탐률〔8〕을 줄여서, 불법적인 우회접속에 대한 역추적과 사건의 포렌식 자료의 생성 연구에 기여하고자 한다.

본 논문의 구성은 다음과 같다. II장에서는 WAS를 통한 DBMS 접근 방법 및 역추적 기법을 소개한다. III장에서는 WAS를 통한 공격 형태를 분석하고, IV장에서는 WAS 우회접속 공격자에 대한 역추적 방안을 연구하고, 기존 방식과 비교한다. 마지막으로 V장에서 결론과 향후 과제에 대해서 논한다.

Ⅱ. 관련 연구

2.1 WAS

기업의 중요자원 시스템과 인터넷을 통한 웹 사이에 위치하면서, 웹 기반 분산 시스템 개발을 쉽게 도와주고 안정적인 트랜잭션 처리를 보장해 주는 미들웨어 소프트웨어 서버의 일종이다. 3-Tier 웹 컴퓨팅 환경에서 기존 클라이언트/서버 환경의 애플리케이션 서버와 같은 역할을 하며, 클라이언트와 서버 환경에서 트랜잭션 처리 및 관리와 다른 기종 시스템 간의 애플리케이션 연동 등을 주된 기능으로 하고 있다.

2.2 WAS를 통한 DBMS 우회접속 기법

2.2.1 DBMS 접속 유형별 분류

DBMS에 접속하는 형태를 유형별로 보면, 그림 2와 같이 크게 4가지 유형으로 나뉜다.

먼저, ①의 2-Tier 접속은 사용자가 DBMS로 직접 접속하는 방법으로 인가된 사용자의 접근경로 이며, ②의 Console 접속 또한 사용자가 콘솔에서 DBMS에 직접 접속하는 방법으로 인가된 사용자의 접근경로 이다. ③의 3-Tier 접속은 Application을 사용하거나, WAS를 통해 DBMS에 접속하는 방법으로 인가되지 않은 불특정 다수의 사용자 접근경로 이다. ④의 우회 접속은 다른 서버를 통해 우회하여 DBMS에 접속하는 방법으로 인가된 사용자 및 인가되지 않은 사용자의 접근경로 이다.

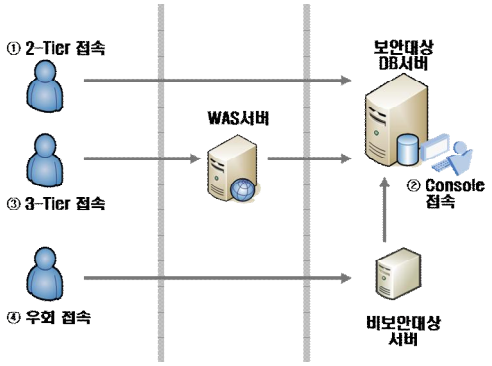

그림 2. DB 접속 경로
Fig 2. DB Connection Path

2.2.2 WAS를 통한 DBMS 우회 접속과 보안 방법

클라이언트/서버 환경에서 웹 환경으로 전환되면서 WAS를 통한 DBMS 접속이 늘어나고 있다.

그림 3. DB보안 이슈의 변화
Fig 3. Change of DB Security Issue

2000년대 초에 감사데이터 생성을 목적으로 sniffing 형태의 제품이 개발되어 유용하게 사용되기는 하였으나 100% 로깅이 불가하다는 한계점이 있다. 2000년대 중반부터 gateway 방식의 DB접근통제 시스템은 Loss가 없다는 장점뿐만 아니라 DB보안에 필요한 정책을 부여해 보안을 한층 강화시키는 방법이다[6][12]. 또한 사용자 개개인의 인증을 위해 Virtual ID를 부여하는 방법과 SQL결재관리를 통해 사용자의 통제 또한 업그레이드 하였다.

이후 불특정 다수의 DB조회 결과에 대한 통제의 필요성이 대두되어 중요 정보에 대해서는 Data masking 기술을 통해 유출을 방지하도록 설계[16][17]하였다. 이 또한 DB조회 결과에 대한 내용으로 DB서버에 저장되어진 상태에서의 보안취약점은 존재한다. 예방책으로 DBMS 서버에 저장 시 중요정보에 대해서는 반드시 암호화해서 보관하라는 지침이 내려지기도 한 상태이다[3].

최근의 DBMS 보안 이슈는 그림 4와 같이 WAS를 통해 비정상적으로 DBMS에 접근하는 우회접속자들에 대한 정확한 로깅이다. DBMS와 WAS 사이에 실제사용자를 식별하는 방법은 기술적으로 한계에 봉착되어 있다[15].

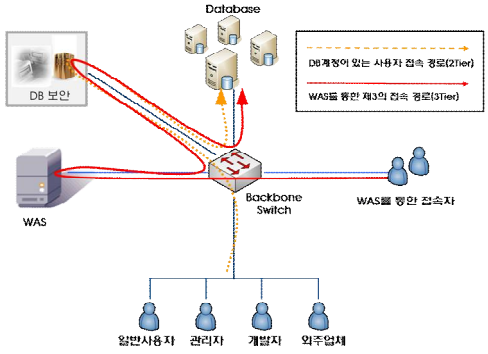

그림 4. DB보안 이슈의 변화
Fig 4. Change of DB Security Issue

2.3 역추적 기법

역추적(Traceback)이란 해킹을 시도하는 해커의 실제 위치를 실시간으로 추적하는 기술로 역추적 기술의 정의와 분류 그리고 역추적 기법[18]의 문제점에 대해 살펴본다.

2.3.1 TCP 역추적 기법

TCP 연결 역추적 기술은 호스트 기반 연결 역추적(host-based connection traceback) 기술과 네트워크 기반 연결 역추적(network -based connection trace back) 기술로 그림 5와 같이 H0에서 Hn까지의 연결들의 집합을 연결체인이라고 한다. 즉, 해커가 실제로 위치한 시스템으로부터 여러 시스템을 경유하여 실제 공격을 당하고 있는 시스템까지의 연

결들의 집합을 말하는 것으로 다음과 같이 정의된다[11].

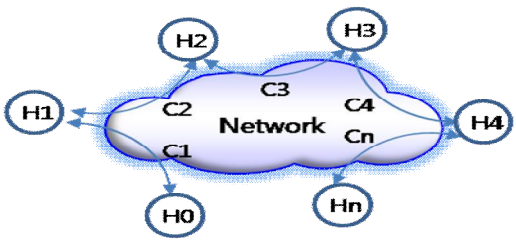

그림 5. 연결체인
Fig 5. A connection chain

2.3.2 Host 기반 역추적 기법

호스트에서 발생하는 로그 기록 등의 다양한 정보를 바탕으로 역추적을 진행하는 기술로 역추적을 수행하기 위해서는 모든 호스트에 역추적 모듈이 설치되어야 하고, 1개의 시스템에서라도 어떤 문제가 발생하면 역추적이 불가능하게 되는 단점을 가지고 있다.

2.3.3 네트워크 기반 역추적 기법

송수신되는 패킷들로부터 역추적을 수행하는 것으로 패킷으로부터 어떤 정보를 활용해야 공격 연결과 같은 연결에 속하는가를 판단할 수 있을지에 대한 알고리즘만이 제기되고 있는 상황이다[9][10].

2.3.4 IP 패킷 역추적 기법

IP 주소가 변경된 패킷의 실제 송신지를 역추적하는 기술로 DoS(Denial of Service)공격, DDoS (Distributed Denial of Service)공격은 변경된 IP 주소 패킷을 악의적으로 사용되는 경우가 대부분이다[13][14]. IP spoofing 해킹 기법을 이용할 경우, TCP sequence number guessing 과정이 필요하며, 공격하고자 하는 대상 시스템에 백도어를 설치하였다[4].

III. WAS를 통한 DBMS 우회접속과 공격 분석

WAS를 통한 DBMS에 우회접속하는 경로상에서 발생할 수 있는 공격형태는 그림 6과 같이 WAS 서버가 설치되어 있는 네트워크 구간에 DoS/DDoS 공격을 하는 네트워크 공격 형태와 공격자가 DBMS 사용자 권한을 획득한 후 WAS를 통해 우회 접근하여 공격자의 정보를 남기지 않고 중요정보를 유출시키는 공격이 있다.

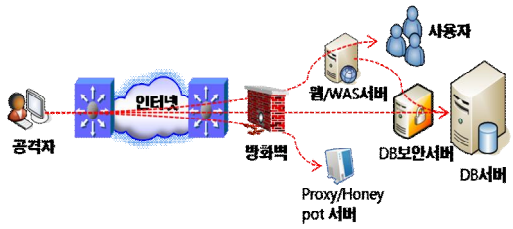

그림 6. WAS를 통한 접속 형태
Fig 6. WAS Attack Type

3.1 WAS 네트워크 공격

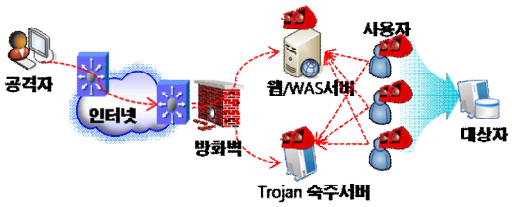

그림 7. DDoS 공격 형태
Fig 7. DDoS Attack Form

DoS 공격을 통하여 네트워크에 한꺼번에 대량의 정보를 보내 허용하는 대역폭을 감소시키거나 공격대상 시스템의 자원을 고갈시켜 서비스의 가용성을 축소시키도록 공격한다.

DDoS 공격으로는 TCP(Syn, Null, Fin, Ack, Push, ResetUgt, Xmas) 공격과 Checksum(TCP, UDP, IP), ICMP 공격, 봇(Bot)을 이용한 공격을 실시한다.

봇(Bot) 공격으로 그림 7과 같이 운영체제의 취약점, 웜·바이러스의 백도어 등을 이용해 전파되는 프로그램이나 실행코드, 명령 전달 사이트와 백도어 연결을 통해 스팸메일 전송으로 봇과 좀비로 감염시킨 호스트들을 이용하여 공격한다.

3.2 WAS를 통한 DBMS 서버 우회접근

그림 8은 DB 보안시스템을 통해 접근 및 권한제어가 구현되어있는 3-Tier 형태의 DBMS 접근경로이다. 172.22.26.39의 내부사용자가 네트워크를 통해 172.22.26.96의 WAS를 경유해 172.22.26.200의 DB보안 Gateway 서버의 정책에 의해 172.22.26.201의 DB서버로 login하게 된다. 이때 DB보안서버는 자체 DB를 통해 로그정보를 저장하게 된다.

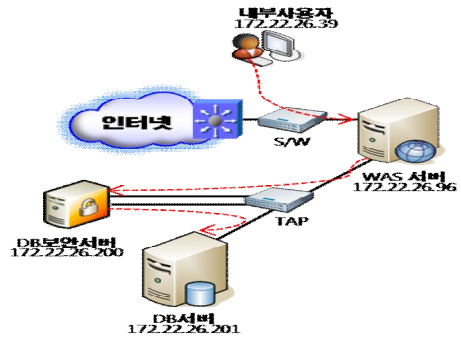

그림 8. WAS를 통한 DB접근
Fig 8. DB access through WAS

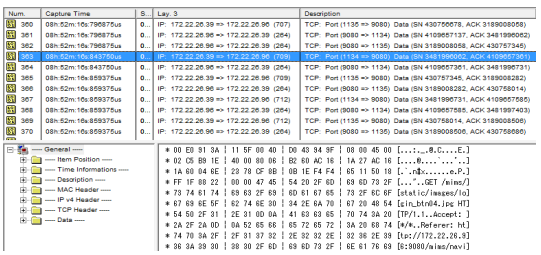

그림 9. 사용자와 WAS의 패킷정보
Fig 9. User and WAS's packet information

테스트장비를 통해 실험한 결과를 경로별로 구분하여 확인한 후 최종 로그데이터를 분석하여 문제점을 확인한다. 그림 9에서는 172.22.26.39의 사용자가 1134번 포트를 통하여 172.22.26.96의 WAS서버 9080으로 정보를 요청한다. 그림 10에서는 사용자의 요청에 의해 172.22.26. 96:1448의 WAS을 경유하여 필요한 정보를 얻기 위하여 172.22.26.200:4001의 DB보안서버로 쿼리를 전달한다.

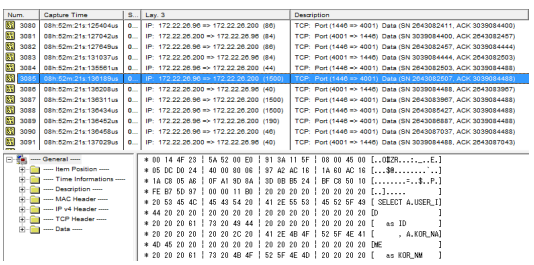

그림 10. WAS와 DB보안서버의 패킷정보
Fig 10. WAS and DB security server's packet information

그림 11에서 DB보안서버는 로그를 남기고 172.22.26. 201:1526의 DBMS로 쿼리를 전달하고 역순으로 결과 값이 전송된다.

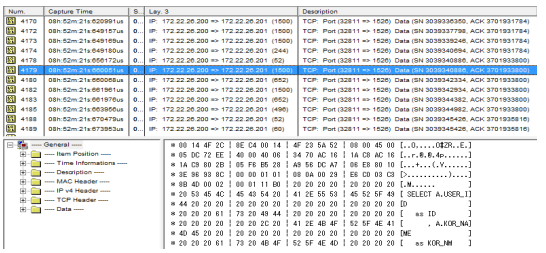

그림 11. DB보안서버와 DB서버의 패킷정보
Fig 11. DB security Server and DB server's packet information

그림 8과 같은 경로로 DBMS에 접근하게 되었을 때 DB 보안서버는 감사를 목적으로 IP, 시간, 포트 등의 정보를 Log 기록으로 남겨 무결성을 확보한다.

No	Type	User ID	User IP	Service	Server
1	DBMS	ressown	172.22.26.96	Test_DB [1]	172.22.26.201 [1526]
2	DBMS	ressown	172.22.26.217	Test_DB_202 [2]	172.22.26.202 [1526]
3	DBMS	exssown	172.22.26.217	Test_DB_202 [2]	172.22.26.202 [1526]
4	DBMS	ressown	172.22.26.217	Test_DB_202 [2]	172.22.26.202 [1526]
5	DBMS	ressown	172.22.26.217	Test_DB_202 [2]	172.22.26.202 [1526]
6	DBMS	ressown	172.22.26.217	Test_DB_202 [2]	172.22.26.202 [1526]

그림 12. DBMS 세션 정보
Fig 12. Session information

Command	Result	User ID	User IP
INSERT INTO TBT01IH106(system_use_seq, use...	Run Complete	ressown	172.22.26.96
SELECT SQ_TBT01IH106_01.NEXTVAL AS syste...	Run Complete	ressown	172.22.26.96
SELECT SQ_TBT01IH106_01.NEXTVAL AS syste...	Run Complete	ressown	172.22.26.96
SELECT a.install_force_cd , (select de,..	Run Complete	ressown	172.22.26.96
set isolation to committed read	Run Complete	ressown	172.22.26.96
set isolation to repeatable read	Run Complete	ressown	172.22.26.96
SELECT DISTINCT COM_PARTI_CD ...	Run Complete	ressown	172.22.26.96
SELECT REG_DTIME, REGR_ID, USE_YN ...	Run Complete	ressown	172.22.26.96
set isolation to committed read	Run Complete	ressown	172.22.26.96
set isolation to repeatable read	Run Complete	ressown	172.22.26.96
INSERT INTO TBT01IH106(system_use_seq, use...	Run Complete	ressown	172.22.26.96
INSERT INTO TBT01IH106(system_use_seq, use...	Run Complete	ressown	172.22.26.96

그림 13. DBMS 세션 정보
Fig 13. Session information

그림 12와 그림 13에서 보면 공격자가 WAS를 경유해서 DB로 접근을 시도했을 때 DBMS 보안서버에 저장되는 IP, 시간, 포트 등의 패킷 정보는 출발지가 사용자가 아닌 WAS 임을 확인 할 수 있다.

IV. DBMS WAS 우회접속 쿼리정보 역추적 연구

3장에서 실험된 접속의 내용에서 실제 접속자의 IP를 확

인할 수 없다는 문제점이 존재한다. 본 논문에서는 WAS를 통해 접속하는 정형적인 중복 쿼리 축약 기술을 통해 해결하도록 제안한다.

4.1 지능형 DB보안 관리시스템 구성도

OLAP(On-line Analytical Processing)/WAS를 경유하여 웹 login한 사용자에 대한 세션/쿼리 정보와 DB보안서버에서 로깅하는 쿼리 정보에 대해 time stamp와 쿼리를 매핑하여 실제 사용자를 식별한다.

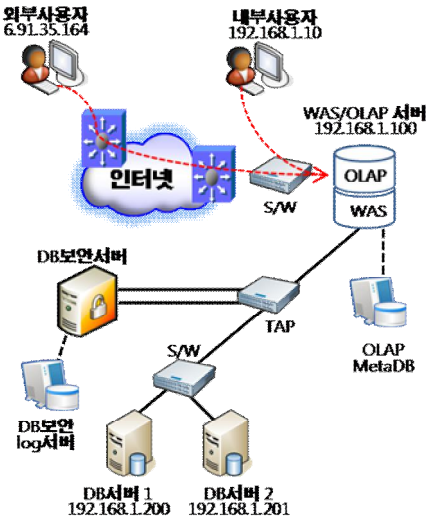

그림 14. 지능형 DB보안 관리시스템 구성도
Fig 14. Intelligence style DB security administration system schematic diagram

그림 14에서 보는바와 같이 내/외부 사용자가 OLAP/WAS 서버를 경유할 때 서버 내에 설치된 별도의 DBMS를 통해 IP, ID 등의 정보를 저장한다. 저장된 정보는 Batch 처리하여 정제된 DB를 DB보안로그서버로 전송한다. DB보안서버를 통해 DB서버로 접근하는 과정에서의 로그는, DB보안로그서버를 통해 패킷정보를 저장한다. DB보안로그서버에 저장된 두 종류의 로그를 gathering 작업을 통해 보안 정책 및 감사 자료로 활용한다.

이때 성능이 떨어지는 단점이 발생함으로 로깅되는 내용은 OLAP/WAS서버의 IP, ID에 대해 사용 SQL과 Return 데이터 값만 로깅한다. OLAP/WAS서버와 DB보안서버의 로그는 기록되는 시간이 약간의 오차가 발생할 수 있다. 테스트 결과에 의하면 거의 동일하거나 약 1분 이내의 오차범위 내에서 발생한다. 그래서 실시간처리는 사실상 어렵고 1일 몇 번을 정하여 Batch Job으로 처리해야 한다.

4.2 지능형 DB보안 관리시스템 구축

WAS를 통한 접속자에 대해 접근 제어 및 감사에 대한 보안 정책설정은 정확성이 떨어지고, 직접접속 보다는 시간도 많이 소요된다. 이러한 문제점은 중복적인 쿼리를 정제하여 축약하는 기술과 정형쿼리를 파싱하는 기술로써 해결할 수 있다. 성능문제를 보완한 지능형 DB보안 관리시스템은 다차원 분석을 통해 지능적인 DB접근통제 및 사후감사의 오탐률을 최소화 한다.

4.2.1 중복 쿼리 축약

WAS에 대한 정형쿼리 및 비정형 쿼리가 중복되어 log 데이터의 유실 및 속도 저하를 야기한다. 그림 15와 같이 기존 방식은 WAS를 통해 접근하는 쿼리에 대해 동일하거나 비슷한 쿼리문을 지속적으로 로깅하여 불필요한 데이터를 저장하게 되는 문제점이 있다.

No	Action	Query	Request Time	Query Count	RT
100001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
98001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
96001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
94001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
92001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
90001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
88001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
86001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
84001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(
82001	Permit (3등급)	SELECT * /* qqq */ FROM DUAL	2008-12-15 16:08:31	2000	59(

그림 15. WAS에 대한 중복 쿼리 결과
Fig 15. Repetition query result

불필요한 로그데이터를 정제되지 않은 상태로 저장하는 것은 과다 트래픽으로 인한 로그데이터 유실, 서버 CPU 부하로 인한 처리속도 저하 현상, 로그감사기록 기능저하로 인한 보안의 취약점 등이 발생될 수 있다.

본 논문에서는 이러한 문제점을 해결하기 위해 중복 쿼리를 축약할 수 있는 기술을 연구하여 초당 10,000 쿼리 발생 시에도 임시 버퍼 파일이 발생하지 않으면서도 100% 처리가 가능하며, CPU 부하를 줄여서 Sniff 서버의 로그 유실을 최소화 한다. 즉 WAS를 통해 접근하는 패턴을 보면 거의 동일한 패턴이다. 이러한 정형 쿼리를 통해 정책을 설정한다. 먼저 log 발생 시 최초 log는 바로 DB에 저장한다. 다음 중복 log는 10초에 한번씩 Count값만 갱신하며, 중복 log라도 1분에 한번은 새로운 log를 기록한다. 중복이란 기본적으로 IP, ID, Application, 쿼리가 같고 1분 이내 실행된 쿼리를 말한다.

여기서 중요한 기술은 정형화 과정이다. 중복되는 로그를 정형화 하는 방법은 주석 및 상수제거, 대소문자, /t, Space

등을 무시하는 것이다.

표 1. 중복 쿼리문의 예
Table 1. Repetition query inquiry example

구분	쿼리문	중복사유
1	Select :1 from dual	상수
2	Select :2 from dual	상수
3	Select /*abc*/:1 from dual	주석
4	SELECT :1 FROM DUAL	대소문자
5	Select ___:1 from dual	스페이스

표 1은 중복 쿼리문의 예 이고, 중복 쿼리문을 일반화 하는 과정은 다음과 같다.

- 주석제거- "/* ~~~ */", "-"표현된 주석을 제거한다.
- 대/소문자 무시-SQL 명령에 대해 소문자로 변환한다.
- 상수 제거-공백, 숫자(정수, 실수, Hexa, Deciamal), single/double quotation mark 또는 "(,)"로 포함된 문자열 등을 제거한다.
- 잘라내기(Trim) 처리-문자열 마지막의 SPACE, TAB, CR/LF등의 제거를 통해 SQL 명령어를 정리한다.

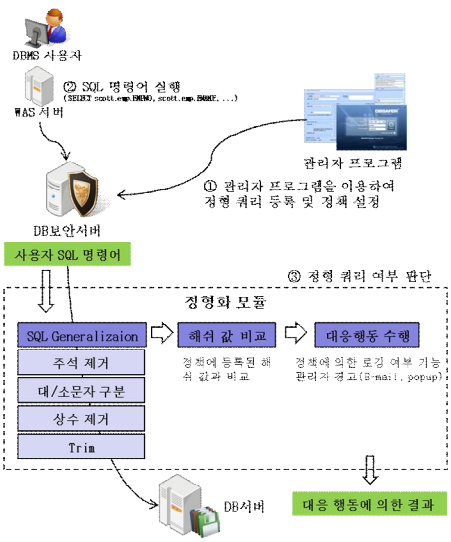

그림 16. 정형 쿼리 탐지 과정
Fig 16. Fixed form query detection process

이렇게 일반화된 SQL 명령어에 대해 SHA-1 알고리즘을 적용하여 해시값을 구한다. 구한 해시값과 정형 쿼리로 등록된 해시값을 비교하여 일치하면 정형 쿼리이며, 그렇지 않으면 비정형 쿼리로 간주한다.

정형 쿼리의 탐지과정 그림 16과 같이 "SQL 명령어 추출" -> "쿼리 일반화(Query Generalization)" -> "해시값 추출(SHA-1)" -> "등록된 정형 쿼리 해시값 비교" 과정을 거쳐 정형 쿼리 여부를 판단한다.

4.2.2 정형 쿼리의 파싱

WAS를 통해 3-Tier로 DBMS에 접근하는 방식의 기존형태는 WAS에 Agent를 설치하여 DB보안서버와의 통신을 통해 자료의 정합성을 일치시키는 방식을 취한다. 이러한 방식은 Agent를 설치해야하기 때문에 WAS의 변경사항이 필수적으로 발생한다. 또한 Agent와 DB보안서버간의 통신이 발생하므로 WAS에 성능 문제가 발생한다.

WAS를 통한 쿼리는 거의 대부분이 정형쿼리이다. 정형쿼리에 대한 파싱작업이 이뤄지지 않으므로 패턴이 다른 동일 쿼리가 들어와도 각각의 쿼리로 인식이 되어 저장 용량이 커지게 된다. 또한 자료의 비교 시 많은 양의 쿼리를 비교해야 하므로 성능에 영향을 미치게 된다.

4.2.3 시스템 아키텍처

지능형 DB보안 관리시스템을 통해 다차원 분석 기능 및 DBMS 접근 기록 검색 기능을 제공하며, 웹 Log, SQL Log를 받아 Pattern을 분석하고, Rule을 만들어 적용은 Module을 개발한다. 그리고 정보 수집 및 정보 압축 실시 후에 DBMS에 보관한다. 보관된 정보는 지능형 DB보안 클라이언트를 이용한 분석과 정책 기반 관리 모듈의 통제를 통해 사후 감시 추적의 오탐률을 적게 할 수 있다.

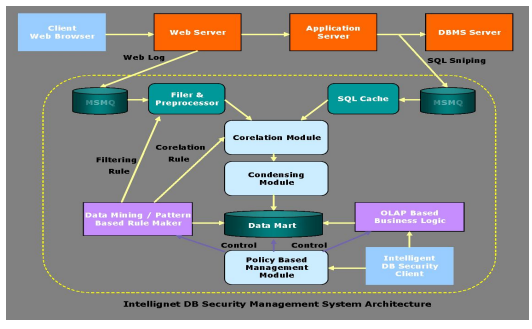

그림 17. 지능형 DB보안 관리시스템 아키텍처
Fig 17. Intelligent DB Security Management System Architecture

지능형 DB보안에 대한 관리시스템 아키텍처는 그림 17과 같으며, 아키텍처 구성은 다음과 같다.

■ 지능형 DB보안관리 클라이언트

사용자별, 시간대별, 테이블별, SQL유형별 다차원 분석 기능 및 DB 접근 기록 검색 기능을 하는 클라이언트를 설치한다.

■ Data Mining / Pattern 기반 Rule Maker

웹 Log, SQL Log를 Data Mining Engine으로 Corelation Pattern을 분석하여 Filtering Rule과 Corelation Rule을 생성한다.

■ Corelation Module

정제된 웹 Log 데이터와 SQL Log들을 받아 Corelation Rule을 적용하여 접속자, 접속IP, 접속시간, SQL로 구성된 레코드를 구성한다.

■ Condensing Module

SQL 유형 식별, 변수 추출, Table 추출 등을 통해 데이터 압축 기능 제공하는 Module을 구성한다.

■ Data Mart

다차원분석 및 데이터 마이닝을 처리하기 위해 Star 스키마 형태로 압축 데이터를 저장한다.

■ OLAP 기반 비즈니스 로직

클라이언트에게 다차원 분석 기능과 DBMS 접근 기록 검색 기능을 제공하기 위한 서버 모듈을 구축한다.

■ Policy 기반 관리 모듈

Policy를 기반으로 Data Mining Training 주기 관리, Data Mart의 데이터 관리, OLAP엔진의 Cube 생성 주기 등을 관리하는 모듈을 구성한다.

4.3 기존 방식과의 비교

표 2. 기존 방식과의 제안 방식의 비교분석
Table 2. Comparative analysis with existing way

구분	기존 방식	논문 제안 방식
Agent 설치	- WAS에 Agent 설치 - DB보안서버와 통신 자료의 정합성 일치	- WAS에 로그 저장으로 Agent 미설치 - DB보안서버 로그와 비교하여 자료 정합성 일치
Application 수정/변경	- Agent 활동으로 CPU memory 등 가용성 축소 - DB보안서버와 통신으로 WAS에 성능 문제 발생	- Agent 미설치로 변경사항 없음 - WAS에서 남기는 로그를 별도의 서버로 전송시키는 Embeded module 필요
네트워크 성능	- 중복쿼리 해결방안이 없으므로 가용성, 트래픽 성능 저하 및 저장 용량 커짐	- 정형쿼리에 대한 중복쿼리 축약 기능 구현으로 성능저하 방지 및 저장 용량 감소
proxy 서버	- proxy 서버 없음	- WAS와 Meta DB서버, DB보안서버와 DB 보안로그서버 각각의 proxy 서버 가동

표 2는 기존의 DBMS보안을 위한 WAS 우회접속자 에 대한 방식과 본 논문에서 제안하는 방식을 비교하였다. 성능 및 기능 테스트 결과는 다음과 같다. 테스트 환경으로 3대의 대상 서버를 192.168.2.128:1521, 192.168.2.237:1522, 192.168.2.239:1521로 셋팅하고, 각각 30개씩, 총 90개 세션에서 동시에 쿼리를 발생시켰다. 전송 쿼리는 "select * /* WAS_SESSION-N */ from dual" 이고, 초당 19,000에서 19,500 쿼리, 총 3,600,000개 쿼리 전송했다.

4.3.1 기존방식의 테스트 결과

기존방식으로 테스트한 결과 그림 18과 같이 로그 조회에서 모두 90개의 세션이 나타났다. 스트레스 테스트 프로그램에서 각각 30개의 세션이 모두 분리되어 기록되었다. 로그조회 결과는 총 3,600,000건의 쿼리 로그가 조회되었고, 쿼리 로그 별 3,000~40,000건씩 축약되었다.

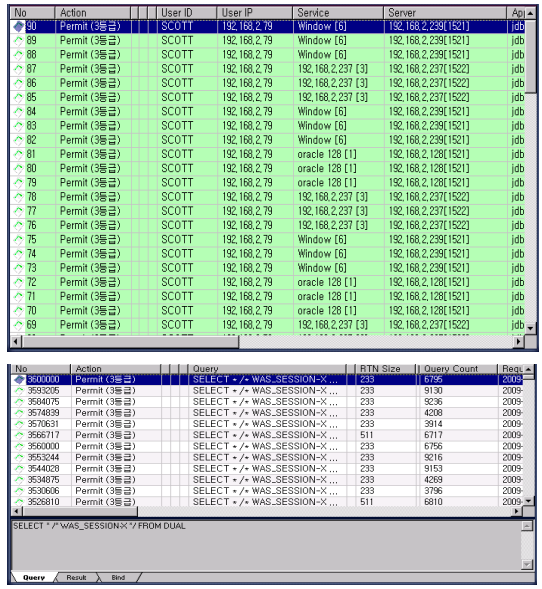

그림 18. 기존방식 테스트 결과
Fig 18. Existing method test result

4.3.2 개선된 방식의 테스트 결과

반면 본 연구를 통해 개선된 방식으로 테스트한 결과 그림 19와 같이 로그 조회에서 모두 8개의 세션이 나타났다. 각각의 서비스별 ***_ora의 fork 데몬의 수(default 3개) 이하로 세션이 축약되었다. CPU 부하량의 변화는 1%미만 이었고, 실 환경에서 query 몇 개 마다 새로 세션이 맺어지는 경우 CPU 감소 효과가 더욱 크게 나타났다. 로그측면에서도 세션은 서비스 데몬의 수와 비례하여 축약되었고, WAS에서 쿼리를 보낼 때마다 새로 접속하는 구조의 경우 기존에는 로그 축

약의 효과가 없었으나, 개선 후에는 세션에 상관없이 로그가 축약되었다. 로그조회 결과도 쿼리 로그 별 15,000~350,000 건씩 축약되어서 로그 축약 성능은 기존 대비 5배 이상의 차이를 보였다.

그림 19. 개선된 방식 테스트 결과
Fig 19. Improvement method test result

V. 결론

본 논문에서 연구의 핵심은 DB보안 로그서버에서 로깅 되어지는 WAS의 IP, ID, 쿼리문, 시간 등의 패킷과 OLAP/WAS에서 Embeded module을 통해 전송된 IP, ID 등의 패턴을 매칭하여 DB보안 로그서버에 정제된 DB를 축적하고, 축적된 DB를 기반으로 정책 Update 및 감사자료로 활용하여 우회접근하는 공격자들을 지능적으로 통제하고 추적하는 기술이다.

또 위의 기술을 적용했을 때 발생하는 성능에 대한 문제로 WAS를 통해 DBMS에 접근하는 형태의 정형쿼리의 중복을 일정시간 동안은 하나의 쿼리로 인식하여 횟수로만 기록, 관리한다. 이러한 중복쿼리 축약 기술을 통해 로그데이터 유실 및 서버 CPU 부하로 인한 처리속도 저하 현상을 방지하고, 정제된 로그데이터를 활용하여 향상된 감사기능으로 보안의 취약점을 해소할 수 있다.

향후 연구 목표는 sniffing의 구조상 발생할 수 있는 일부 패킷 유실과 저장시간 범위의 차이에 따라 발생할 수 있는 오탐률을 완벽히 제거하기 위한 로그 검증 및 위변조 방지 기술을 연구하여, DBMS 보안을 위한 무결성 입증에 이바지할 것이다.

참고문헌

〔1〕 한국정보보호진흥원, "*인터넷침해사고 동향 및 분석 월보*," *http:// www.krcert.or.kr*, 2008년 12월.

〔2〕 김정보통신부, "*정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령*", 대통령령 제20668호, 2008년 2월.

〔3〕 교육과학기술부, "*교육과학기술부 및 교육·연구기관의 개인정보관리 업무편람*, 85쪽, 2008년 5월.

〔4〕 Belenky A. and Ansari N., "IP traceback with deterministic packet marking," Communication Letters, IEEE, Vol. 7, Issue 4, pp. 162-164, Apr. 2003.

〔5〕 김정상, "*개인정보 침해사례를 통한 데이터베이스 보안에 관한 연구*", 건국대 정보통신대학원, 2007년 6월.

〔6〕 이강석, "*데이터베이스 사용자 사전 통제 및 사후 추적을 통한 데이터베이스 보안 연구*, 한양대 공학대학원, 2007년 2월.

〔7〕 금융결제원, "*DB보안 기술의 현황과 문제점 분석*," Information Security Conference 2007, 2007년 9월.

〔8〕 박천오, "*지능형 DB보안 관리시스템 개발 계획서*," 피앤피시큐어, 2007년 5월.

〔9〕 이직수, "분산 서비스 공격 대응을 위한 역추적 시스템 개발," 한국정보처리학회논문지, 제12권, 2호, 1067-1070쪽, 2005년 11월.

〔10〕 채철주, "IP 역추적 기술을 이용한 실시간 역추적 시스템 설계 및 구현," 한국정보처리학회논문지, 제14권, 1호, 1133-1136쪽, 2007년 5월

〔11〕 이인희, "IP 역추적 설계 및 보안감사 자료생성에 관한 연구," 한국컴퓨터정보학회논문지, 제15권, 1호, 53-64쪽, 2007년 6월.

〔12〕 문형진, "역할기반 접근제어시스템에 적용가능한 민감한 개인정보 보호모델," 한국컴퓨터정보학회논문지, 제13권, 5호, 103-110쪽, 2008년 9월.

〔13〕 윤병선, "우회적인 공격에 대한 실제 IP 역추적 실시와 포렌식 자료 생성," 한국컴퓨터정보학회논문지, 제13권, 1호, 143-151쪽, 2008년 1월.

〔14〕 Tsern Huei Lee, Wei-Kai Wu, Tze-Yau William

Huang, "Scalable packet digesting schemes for IP traceback," 2004 IEEE International Conference , Vol. 2, pp. 1008-1013, June 2004.
〔15〕 문승재, "*안전한 DB 보안을 위한 레이블 세션유지 방안 연구*," 숭실대학교 정보과학대학원, 2008년 6월.
〔16〕 백종일, "*데이터베이스 보안을 위한 가용성 확장 연구*," 숭실대학교 정보과학대학원, 2008년 12월.
〔17〕 백종일, "DB 보안의 문제점 개선을 위한 보안등급별 Masking 연구," 한국컴퓨터정보학회논문지, 제14권, 4호, 101-109쪽, 2009년 4월.
〔18〕 Dea-Woo Park, "*A Study on Problem of Korean-Digital Forensic*," International Conference on Ubiquitous Information Technologies & Application, ICUT (1976-0035), Dec. 2008.

저 자 소 개

백 종 일

2005: 한국방송통신대학교 미디어 영상학과 (공학사).
2009: 숭실대학교 정보과학대학원 정보보안학과 (공학석사).
2009 - 현재: 호서대학교 벤처전문대학원IT응용기술학과 (박사재학)
2009 - 현재: (주)조은아이앤에스 정보보안팀 팀장
관심분야 : DataBase보안, 정보보호, DB 포렌식, 정보보호 시스템, 유비쿼터스 보안 등

박 대 우

1998: 숭실대학교 컴퓨터학과(공학석사)
2004: 숭실대학교 컴퓨터학과 (공학박사)
2000: 매직캐슬정보통신 연구소 소장, 부사장
2004: 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006: 정보보호진흥원(KISA) 선임연구원
2007: 호서대학교 벤처전문대학원 조교수
관심분야: 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, IT-Convergence