VM(Virtual Machine)을 이용한 분리된 가상화 침해유형 학습 데이터베이스 관리와 보안방안

정회원 서 우 석*, 전 문 석*

The Management and Security Plans of a Separated Virtualization Infringement Type Learning Database Using VM (Virtual Machine)

Woo-seok Seo*, Moon-seog Jun* *Regular Members*

요 약

최근 지속적이고 치명적인 데이터베이스에 대한 공격성향은 보안 정책과 유사한 발전형태를 가지고 비례적으로 진보하고 있다. 폐쇄적 네트워크에서 생성된 정보에 대한 접근제어 기반의 방어기법과 제한된 접근경로에 대한 공격을 과거 축적되고 학습되어진 공격패턴을 기반으로 많은 시스템과 데이터베이스가 침해당하는 사례가 늘고 있다. 따라서 본 논문 연구를 통하여 제한된 인증과 접근권한에 대한 안정성 확보를 위해 이원화된 VM(Virtual Machine)을 탑재한 가상 침해 패턴 시스템 기반으로 공격정보와 형태를 분리하고 공격 네트워크에 대한 침해 패턴 집중관리를 통해 침해를 차단하는 시스템을 제안하고 최종 데이터베이스를 방어하는 실험과 최적의 방어 기법 및 보안 정책을 구현하기 위한 메커니즘을 개선코자 한다.

Key Words : Virtual Invasion Pattern Defense System, VM, DB, Security Policy, Access Control, Attack Flow

ABSTRACT

These days, a consistent and fatal attack attribute toward a database has proportionally evolved in the similar development form to that of security policy. Because of access control-based defensive techniques regarding information created in closed networks and attacks on a limited access pathway, cases of infringement of many systems and databases based on accumulated and learned attack patterns from the past are increasing. Therefore, the paper aims to separate attack information by its types based on a virtual infringement pattern system loaded with dualistic VM in order to ensure stability to limited certification and authority to access, to propose a system that blocks infringement through the intensive management of infringement pattern concerning attack networks, and to improve the mechanism for implementing a test that defends the final database, the optimal defensive techniques, and the security policies, through research.

I. 서 론

최근 최적의 시스템을 구현하는 방안으로 자원공유를 기반으로 하는 Virtual Machine("이하 VM이라 칭한다.")이 대두되고 있다. 과거 업무 프로세스별 또는 목적별 분류되어 도입되고 구축되어진 솔루션을 하드웨어 성능의 비약적인 발전에 따라 하나의 시스템 내에 탑재하고 운영하는 기술이 가장 큰 이슈가 되고 있다. 최초 VM은 목적별 분류에 의해 다수의 시스템에 분산되어진 모듈을 집약적으로 하나의 시스템에 구현

* 숭실대학교 컴퓨터학과(ssws2003@yahoo.co.kr, ijcsns@gmail.com)
논문번호 : KICS2011-05-221, 접수일자 : 2011년 5월 16일, 최종논문접수일자 : 2011년 7월 20일

함으로써 관리적인 측면에서 효율성을 높이는데 국한되어 있었다. 하지만 현재는 서비스별 분류에 따른 VM으로 구현함으로써 여러 곳에 산재해 있던 데이터베이스 관리의 일원화와 방어적인 측면까지 포함되어진 형태로 발전하고 있다. 다만 현재의 데이터베이스의 VM 실현은 특정 모듈에 의해 생성되어진 정보를 대상으로 하지만, 본 논문에서는 생성된 단순 데이터베이스 관리가 아닌 내부 네트워크로 접속 또는 접속을 시도한 정보인 Packet 정보, 네트워크 접속자 정보, 접속 IP 정보 등을 학습한 보안관련 데이터베이스를 VM을 통해서 구현함으로써 외부 침해가 발생 시에도 학습되어진 데이터베이스 정보를 VM을 이용하여 직접적인 공격을 방어하고 VM운영에 대한 표준화 구현 방법을 제안한다[1,2].

본 논문의 구성은 다음과 같다. 2장에서는 최근 네트워크 기반의 단계별 공격유형 분류와 계층별 공격유형, 학습 패턴 구성 데이터베이스 현황을 확인하고 3장에서는 취약점 공격과 침해유형 학습정보를 활용한 침해패턴 관리기반의 방어기법들이 기술되고, 4장에서는 분산된 공격패턴 학습기반의 VM 탑재 데이터베이스에 대한 방어 실험과 결과를 분석하고, 5장에서는 결론을 기술한다.

Ⅱ. 관련연구

2.1 네트워크 기반 단계별 공격유형 분류

과거 치명적인 침해사례를 발생시킨 공격기법과 변이를 통해서 공격이 이루어지는 Zombie형태의 공격기법 중에서 본 논문에서는 우선 수년전부터 현재까지 지속적으로 공격기법으로 활용되어지고 새로운 버전으로의 응용이 이루어진 5가지 공격기법으로 분류하고 각 공격기법마다 이루어지는 하위 공격패턴과 유형을 표 1과 같이 분류했다. 또한, 공격으로 인한 파급 장애 효과가 큰 DoS(Denial of Service)와 DDoS(Distributed Denial of Service attack)로부터 Spoofing, Session Hijacking으로 분류하고 하위 각 분류마다 총 28개의 공격패턴으로 구분했다. 이외의 변이한 공격 패턴들이 있으나 가장 많은 공격 성향과 패턴을 중심으로 기술했다[3].

2.2 TCP/IP 4 계층과 OSI 7 계층별 운영 프로토콜과 공격유형 분류

Public Network에서 운영되어지고 있는 네트워크 기반의 표준화 프로토콜은 TCP/IP 4계층과 OSI 7 계층이 가장 많이 운영되어 지고 있다. 물론 이외의 NetWare 등과 같은 특정 네트워크 프로토콜 기반도 있으나, Public Network을 통한 내부 네트워크에 대한 접속 시점까지는 2가지 형태의 통신규약이 표준화되어 있으므로 그에 따른 계층별 운영 프로토콜과 공격유형으로 분리했다. 표 2는 TCP/IP 4 계층별 운영

표 1. 네트워크 기반 단계별 공격유형 분류

Attack - Section				
Dos / DDoS	Network Scanner	Remote Attack	Sniffing	Spoofing, Session Hijacking
AC	AC	AC	AC	AC
Brute-Force / Inconsistent Fragmentation / Land/ NewTear / Nestea / Ping of Death / Stacheldraht / Syn Flooding / Smurf / Teardrop / Targa / Trinoo / TNF / TFN2K / UDP Flooding	IP Scanner / Port Scanner / Remote Finger Printing / Third Party Effect	Remote Active	ARP Redirect / Hub Attack / ICMP Router Advertise-ment / ICMP Redirect / Switch Jamming	ARP / DNS / E-mail / IP Web
	* AC : Action			

표 2. TCP/IP 4 Layer 계층별 운영 프로토콜과 공격유형 분류

TCP/IP 4 Layer	Level	DB	Protocol	Attack Mode
Application	L4	A	BOOTP, DNS, HTTP, FTP, SMTP, SNMP, SSH, TFTP	Botnet Worm, Cache Control, HTTP Get Flooding, Hacking, RPC, SQL, VOIP
Transport	L3	B	STCP, TCP, UDP	TCP SYN Flooding, TCP Flag Flooding, UDP Flooding
Internet	L2	C	ARP, ICMP, IGMP, IP, RARP	ARP Spooping, ICMP Flooding, IGMP Flooding, IP Flooding, RARP Spooping

프로토콜과 공격유형 분류를 제시한 것이며, OSI 7 계층에 대한 분류는 표 3과 같다[4].

VM기반의 데이터베이스 구현 시에는 운영되는 공격패턴을 기준으로 학습하고 분석하는 과정이 이루어짐으로써 운영 프로토콜을 데이터베이스화 한다. 이때 TCP/IP 4 계층과 OSI 7 계층 정보를 하나의 Query로 구성함으로써 향후 지속적인 VM 기술의 발전에 따라 각각의 분류기준에 따른 학습패턴을 VM으로 구성 가능함으로 전체적인 분석 대상을 계층별 2가지로 구성했다[5,6].

표 3. OSI 7 Layer 계층별 운영 프로토콜과 공격유형 분류

OSI 7 Layer	Level	DB	Protocol	TCP/IP 4 Layer Compare [Attack]	Attack Mode
Application Presentation Session	L7 ~ L5	A'	BOOTP, DNS, FTP, HTTP, SMTP, SNMP, SSH, TFTP	same	Botnet Worm, Cache Control, HTTP Get Flooding, Hacking, RPC, SQL, VOIP
Transport	L4	B'	STCP, TCP, UDP	same	TCP SYN Flooding, TCP Flag Flooding, UDP Flooding
Network	L3	C'	ARP, ICMP, IGMP, IP, RARP	same	ARP Spooping, ICMP Flooding, IGMP Flooding, IP Flooding, RARP Spooping
Data-Link Physical	L2 ~ L1	-	MAC	-	-

2.3 학습 패턴 구성 데이터베이스 현황

방화벽과 같은 보안기기는 실시간 로그를 저장하고 저장한 로그를 재분석하는 과정을 통해서 외부로부터 불법적인 접근시도, 잦은 접근 시도 IP 목록, 패킷 흐름 기록, 분석 정보, 공격 패턴, 계층별 공격 포인트 등 다양한 정보를 보유하게 된다. 물론 학습 되어진 공격 패턴 정보를 분석한 결과에 따라 최적의 방어정책을 설정하기 위해 활용하는 면에서는 본 논문에서 제안하고 실험하고자 하는 이원화된 VM(Virtual Machine)을 탑재한 가상 침해 패턴 시스템과 운영상의 활용은 다를 바가 없다. 하지만 학습 되어진 공격패턴을 방어를 위한 정책에 적용하기 위한 목적별, 기능별, 정책 등급별로 구분하고 각각의 데이터베이스를 구성함으로써 데이터베이스에 대한 직접적인 공격을 받아도 전체 보안정책을 구성하기 위한 정보가 탑재되어진 데이터베이스가 일시에 침해당하지는 않는 차이점을 갖는다. 또한, 침해정보, 분석정보, 보안정책 등과 같은 실시간 생성 및 응용하는 정보를 보유하는 방법으로는 3가지 형태가 있다.

* *단일 데이터베이스 : 네트워크 보안장비 내에 존재하는 기억장치로써 로그 또는 보안정책 설정 정보를 갖는 데이터베이스를 의미*
* *복제 데이터베이스 : 주요 보안을 유지하기 위한 정책과 실시간 로그를 기록하는 주요 기억장치를 1:1로 미러링하는 기능을 가진 데이터베이스를 의미*
* *보안 시스템 데이터베이스 : 외부로부터 불법적인 접근을 차단 및 관제하고 분석하기 위한 네트워크 보안장비를 관제하는 별도의 시스템 내의 데이터베이스를 의미*

Ⅲ. 취약점 공격과 침해유형 학습정보를 활용한 침해패턴 관리기반의 공격과 방어

내부 네트워크로 접근하는 모든 접속관련 정보를 학습하는 VM기반의 분산 데이터베이스를 접속을 시도한 정보인 Packet 정보, 네트워크 접속자 정보, 접속 IP 정보 등의 구분인자를 통해 구분하고 다차원으로 데이터베이스 Query를 VM에 적용하여 분리한다. 공격패턴을 VM으로 구현하고 지속적인 방어기법에 활용하고 해당 정보를 공유하기 위해 방어 시스템과 데이터베이스 부문에 대한 동기화와 동기화에 따른 Load-Balancing으로 취약점 제어가 필요하다. 또한, 논리적 가상 침해패턴 방어 구현으로 직접적인 데이터베이스에 대한 침해를 방어하는 별도의 솔루션 역시 필요하다. 이처럼 2가지 부문에 대한 침해패턴 분산 데이터베이스 집중관리를 위한 방어기반이 우선 적용 및 구현되어야 한다[7].

3.1 동기화 데이터베이스에 대한 취약점과 공격

논리적으로 침해 학습 되어진 분산된 데이터베이스를 최종 하나의 Master 데이터베이스로 구현하는 첫

번째 동기화 과정과 가상 침해패턴 방어 시스템에 최종 데이터베이스를 동기화하는 두 번째 과정에 그림 1과 같이 각각의 취약점인 Synchronization loss time이 발생한다. 동기화 과정에 발생하는 취약점을 공격하는 방법으로는 SQL-Injection 공격 등이 있다.

* *동기화 데이터베이스 : 다수의 보안정책 구현을 위한 학습 패턴이 기록되어진 서로 다른 데이터베이스 간의 실시간 정보유지를 위한 동기화*

Sync_DB={Master_DB||Slave-1_DB||...||Slave-n_DB}

* *동기화 취약점 : 다차원으로 데이터베이스 Query를 VM에 적용하고 분리되어진 자료간의 동기화를 Query 갱신, Query 상호 정보 유지 등의 동기화를 저해하는 공격으로 발생하는 취약점*

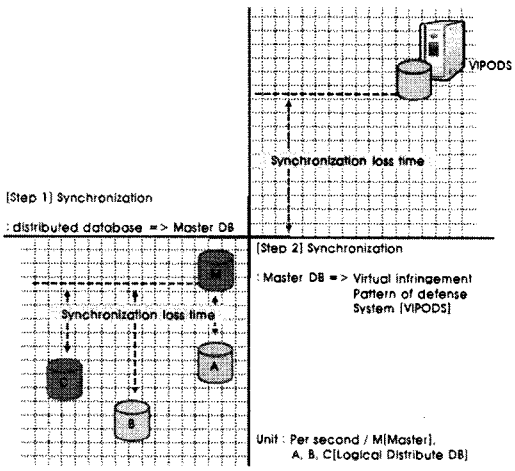


그림 1. 동기화 취약점(Synchronization loss time)

3.2 논리적인 데이터베이스 구현을 통한 VM 기반의 방어

가상 침해패턴 방어 시스템 구현을 위해 VM적용 가능한 시스템 성능을 실험 및 분석하고 그림 2와 같이 2개 이상의 VM을 서로 다른 운영체제를 탑재한 가상 침해패턴 방어 시스템을 구성함으로써 외부 침입자가 판단 시에 하나의 시스템에 하나의 데이터베이스를 공격하는 것 같은 혼동이 발생하도록 1차 구현하고 2차적으로는 Secure OS와 같은 운영체제 보안 솔루션이 탑재되어 혼용되어 운영되어지는 2차적인 데이터베이스 활용 운영체제를 분리함으로써 접근제어를 한다.

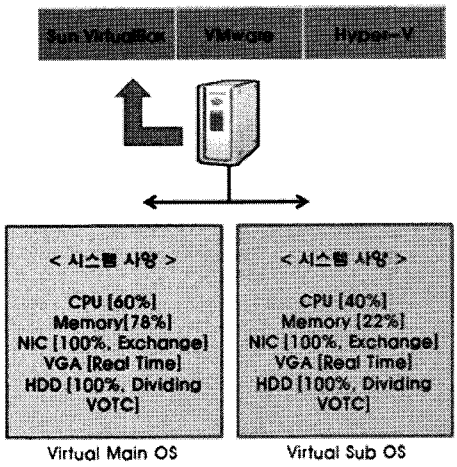


그림 2. 가상 침해패턴 방어 시스템

가상 침해 패턴 방어 시스템의 단계적 구성과 처리 흐름은 총 5단계로 구성되어진다.

1) 공격 인지
2) 공격 패턴 분석
3) VM 기반에 운영중인 학습된 공격 패턴에 따른 데이터베이스 선택
4) 해당 데이터베이스를 실시간으로 보안기기 정책에 반영(업로드)
5) 지속구현

공격의 대상은 Master 데이터베이스이고 Master 데이터베이스의 공격 패턴 학습 정보가 분실 또는 파괴되는 경우 분산되어 있는 논리적인 데이터베이스 조각들이 다시 Master 데이터베이스로 동기화되고 그림 3과 같이 원래의 형태로 복원을 유지함으로써 방어한다. VM을 구현함으로써 다수의 서로 다른 운영체제가 구동되어지고 각 운영체제마다 분류되어진 공격 학습 패턴을 가진 데이터베이스를 구성하고 또한

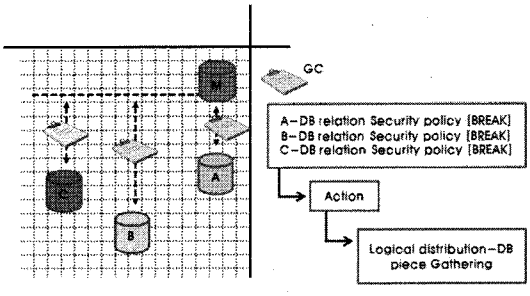


그림 3. 논리적 분산 데이터베이스 조각 모음

방어정책 상에 반영되어진 특정 데이터베이스가 침해로 인해 파괴되거나 동작하지 않는 경우에는 상호 동기화 되어 있는 다른 운영체제 하의 데이터베이스가 실시간 매핑 결과에 따라 손상되어진 데이터베이스 조각을 상호 유지시킨다.

Ⅳ. 이원화된 VM을 탑재한 가상 침해 패턴 시스템 방어 실험

4.1 실험환경

공격을 시행하는 Attack 시스템은 CentOS 기반의 운영체제를 탑재한 서버로 구성하고 공격 학습 패턴 데이터베이스 분리와 구성을 위한 가상화 기법은 VM을 이용하여, 7개로 분리한다. 또한 공격기법은 SQL-Injection 공격을 시행함으로써 각 데이터베이스 구분인자와 Query에 대한 침해 공격을 시행한다. 세부적인 공격에 대한 방어실험으로는 그림 4와 같이 서로 다른 운영체제를 가진 VM으로 목적지 정보를 가진 패킷에 대한 방어정책 설정정보와 학습패턴 정보, 공격 패킷의 흐름 파악 정보, 기록 분석 정보, 세부적인 공격 네트워크에 대한 침해패턴별로 정보 등 논리적인 분산 데이터베이스를 구현하고 또한 전체 데이터베이스를 통합적으로 구현한 침해유형 데이터베이스를 백업으로 구성한다. 이때 계층별 공격유형을 구분해서 접근시 침입유형과 네트워크 영역, IP유형으로 분류하여 각 침해패턴 데이터베이스의 정보를 가지고 방어하는 최종 실험을 함으로써 VM으로 구성한 IP기반의 공격유형 분류 및 방어정책의 효율성을 Query 분석기와 같은 데이터베이스 성능 분석기로 확인한다.

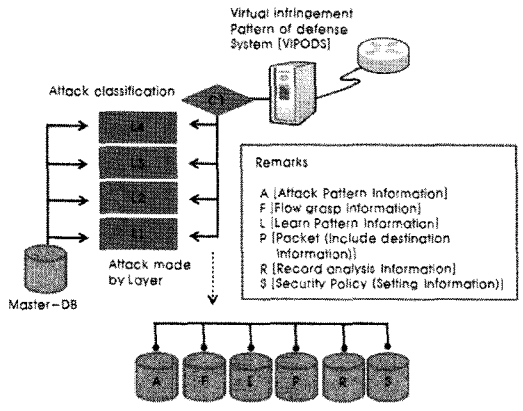


그림 4. 실험환경

4.2 공격에 대한 방어

VM을 통한 동기화 분산 데이터베이스 구현의 경우 그림 5와 같이 분산데이터베이스 개념을 적용하여 하나의 시스템 내에 VM을 구현해서 데이터베이스를 분리 저장함으로써 논리적으로 데이터베이스를 Object 단위로 분리 구성한다. 따라서 침해가 발생하더라도 특정 단위의 구분된 하나의 데이터베이스 조각만이 침해를 입지만, 그 외의 남은 논리적 데이터베이스를 재조합함으로써 1차적인 침해를 방어하고 2차적으로는 해당 공격패턴에 대한 과거로부터 축적되어 분석되어진 데이터베이스를 읽어 들여 해당 패턴에 대처 가능한 방어모듈을 적용한다.

논리적으로 구분된 데이터베이스 조각들이 특정 코드인식 값에 따라 서로 다른 운영체제하에 VM으로 구성됨에 따라 침해되어 잃어버린 논리적 데이터베이스 조각을 남은 데이터베이스 조각으로 재조립함으로써 방어가 가능하도록 별도의 Query 조합정책과 같은 복구 솔루션을 별도로 구성한다. 별도의 분할되어 있는 논리조각인 부분 데이터베이스를 이중화하거나 시스템에 통합 데이터베이스를 구성해서 데이터베이스 침해에 대비함으로써 최적화된 방어가 이루어진다.

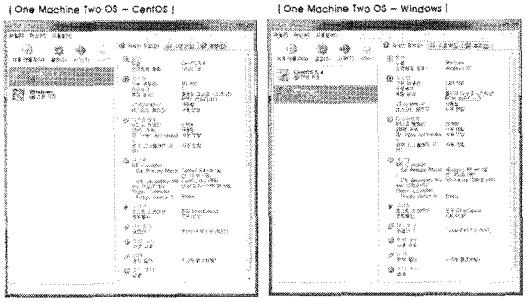


그림 5. 서로 다른 운영체제의 VM 구현

4.3 기존 학습 패턴 데이터베이스 구성 비교

특정 목적과 결과를 필요로 하는 솔루션에 의한 결과값을 정보로 활용하는 데이터베이스와는 보관, 운영, 관리부분에서 성격이 전혀 다른 보안정책과 접근제어 등을 위한 데이터베이스를 구축하는 것이 본 논문의 연구에서 필요로 하는 목적이다. 따라서 업로드와 다운로드와 같은 기능적인 활용보다는 침해 패턴 분석 결과를 기반으로 하기 때문에 이원화된 VM을 이용한 공격 패턴을 데이터베이스로 활용하는 방안을 제안한 것이다.

따라서 기존에 분석과정을 필요로 하고 분석결과를 활용하지 않았던 다양한 데이터베이스 구성과의 비교

표 4. 침해 정보 학습 데이터베이스 구성 비교

구분	제안DB	단일DB	복제DB	보안 시스템DB
VM 탑재여부	○	X	X	X
DB 구성	침 해 비 율 10% 미만 빌생 조건에 따른 DB 구성 제한	1개	2개	보안 네트워크 장비 : 1개 관제 시스템: 1개
동기화 유무	○	X	X	X
DB 조각 모음 유무 [침해로 인한 일부 DB 파손시]	○	X	X	X

를 표 4와 같이 제시함으로써 최적화된 보안을 위한 최적화 데이터베이스 구현 기본조건을 확인한다.

4.4 공격에 대한 결과 분석

실험환경 조건에서 6가지의 분산 방어 데이터베이스를 구현하고 공격으로 침해 받은 논리적 데이터베이스를 Master 데이터베이스로 복구하는 비율을 확인함으로써 표 5와 같이 Defense 비율, 동기화 적정 비율, 정보 분실 비율 등의 결과가 나타났다.

또한 공격 패턴 정보를 너무 많은 데이터베이스로 분리시키게 되면, 그림 6과 같이 오히려 전체 Flow grasp Information과 Record analysis Information 등에 치명적인 10% 이상의 침해 비율이 나타났다. 따라서 VM 기반의 방어를 위한 기본 학습되어진 공격 패턴 데이터베이스는 분리비율을 조율함으로써 가장 최적화된 방어 데이터베이스 구현이 이루어진다.

표 5. 실험결과

DB unit [rate, %]	Attack Pattern Information	Flow grasp Information	Learn Pattern Information	Packet (Include destination Information)	Record analysis Information	Security Policy (Setting Information)]
Defense	97 ~ 98%					
Sync	complete	Delay [1~3%]	complete	complete	Delay [6~11%]	complete
Lose	less than 2%	less than 7%	less than 2%	less than 2%	less than 14%	less than 2%

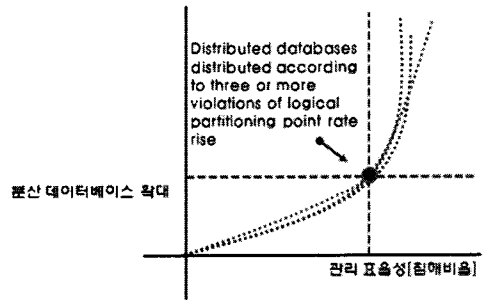


그림 6. 분산 데이터베이스 확대 .vs. 관리효율성(침해비율) 비교

V. 결 론

본 논문에서는 분산 데이터베이스를 논리적으로 각각의 분류기준인 Attack Pattern Information, Flow grasp Information, Learn Pattern Information, Packet (Include destination Information), Record analysis Information, Security Policy (Setting Information)]의 6가지로 분리 구현함으로써 침해에 대한 방어 학습패턴의 데이터베이스 활용 비율과 데이터베이스의 논리적 분산 시와 침해비율에 대해서 알아보았다. 최종 실험결과로는 3개 이상의 논리적 조각 데이터베이스를 기준으로 침해비율의 변환점이 발생함을 확인했다. 향후 연구방향으로는 확장된 VM 실험연구와 최적화 모델에 대한 연구를 데이터베이스 분류 범주기준과 표준화를 위해 더욱 다양한 공격환경 구성으로 실험함으로써 방어의 효율성을 위한 최적의 분산 데이터베이스 표준화를 구현해야 할 필요성과 다양한 데이터베이스 중 가장 보안 방어 학습패턴에 대한 빠른 동기화 모듈을 지원하는 데이터베이스를 선별하는 자동화 학습 실현 프로세스와 표준화 구현을 위한 필요성에 대한 객관적인 평가가 필요하다. 또한, 향후 지속적인 제안 시스템의 연구범위 확장을 위한 객관적인 결과값을 비교 및 검토할 수 있는 연구가 요구된다.

참 고 문 헌

[1] Li Xinlei, Zheng Kangfeng, Yang Yixian, "A DDoS attack defending scheme based on network processor", 2009 WASE International Conference on Information Engineering, pp.238-241, 2009.

[2] Zaihong Zhou, Dongqing Xie, Wei Xiong, "A P2P-based Distributed Detection Scheme Against DDoS Attack", 2009 First International

Workshop on Education Technology and Computer Science, pp.304-309, 2009.

[3] P.Jayashreel, K. S. Easwarakumar, D. Radhakrishnan, N. Lakshmanan, P. Dinakaran, "A Payload driven Security model for flooding attacks in Active networks", 2009 IEEE International Advance Computing Conference, pp.934-939, 2009.

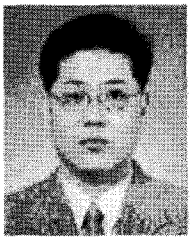
[4] Yusuke Shomura, Yoshinori Watanabe, "A Traffic Monitoring Method for High Speed Networks", 2009 Ninth Annual International Symposium on Applications and the Internet, pp.107-113, 2009.

[5] PENG Yali, Deng Mingxing, Deng Jiangang, YU Min, "Formal Modeling of a Kind of IDS and Research of Its Detection Technology", 2009 First International Workshop on Education Technology and Computer Science, pp.570-573, 2009.

[6] Muhammad Hasan Islam, Kamran Nadeem, Dr Shoab A Khan, "Optimal Placement of Detection Nodes against Distributed Denial of Service Attack", International Conference on Advanced Computer Control, pp.675-679, 2009.

[7] 김미영, 이영록, 이형효, 김용민, "데이터베이스에서 개인정보보호를 위한 정책기반 쿼리 변환기 설계 및 구현", 한국정보처리학회 학술대회, pp.1112-1115, 2008년 5월.

서 우 석 (Woo-Seok Seo) 정회원



2006년 숭실대학교 정보과학대학원 정보통신융합학과 석사

2009년 9월~현재 숭실대학교 컴퓨터학과 박사과정

<관심분야> 정보보호, 네트워크 보안, 방화벽, Router & Network Design

전 문 석 (Moon-Seog Jun) 정회원

1981년 2월 숭실대학교 전자계산학과

1986년 2월 University of Maryland Computer Science 석사

1989년 2월 University of Maryland Computer Science 박사

1989년 3월~7월 Morgan State University 조교수

1989년 9월~1991년 2월 New Mexico State University Physical Science Lab. 책임연구원

1991년 3월~현재 숭실대학교 컴퓨터학과 정교수

<관심분야> 정보보호, 전자여권, 전자상거래