韓國 OA學會 論文誌
第7卷 第2號, 2002. 6.

2002-7-2-1-6

모바일 접근에 의한 정보 누출을 막기 위한 Circuit Patrol 침입탐지 시스템 설계

장 덕 성*

Design of Intrusion Detection System Using the Circuit Patrol to protect against information leakage through Mobile access

Duk-Sung, Jang*

요 약

모바일의 확산, 이동성, 그리고 휴대성은 유선 인터넷의 추세를 점차 무선 인터넷으로 전이시키고 있다. 이에, 기업의 일선 업무 담당자들과 일반인들은 모두 모바일 폰, PDA를 활용하여 지역에 관계없이 이동을 하면서 기업정보와 국가정보에 접근할 수 있게 되었다. 이에 따라 기업정보 도용과 개인정보를 악용하는 경우가 자주 등장함에 따라 정보보호가 사회전반에 큰 이슈화되고 있다. 본 논문에서는 정보보호를 위한 침입탐지 시스템을 설계하고자, 유선 인터넷의 침입 유형과 침입탐지 기법을 살펴보았다. 본 논문은 모바일 무선 인터넷에 의한 시스템 접근 시에 침입을 탐지, 분리하며, 정상으로 가장하여 시스템 내부에 침입한 경우를 탐지하고자 circuit patrol을 시스템 내부에 위치시켜 정상적인 것처럼 시스템에 들어온 침입에 대한 공격을 탐지하는 모델을 제시하였다.

Abstract

Trend of wire internet has been transferred to wireless internet gradually due to the spread of mobile phone which made possible Mobility and portability which wire internet could not afford. Not only front line of business part can access business information but also people can use government information for their daily life without limit of place. The frequent report of larceny and misuse of information has been issued to social sector that the need for IDS considering wire wireless internet. In this paper to design IDS to protect information first, searched wire internet intrusion type, intrusion detection method, and wireless intrusion type. In this paper, first, separate abnormal access at the point of system landing and detect intrusion attack with disguise through mobile wireless internet. Due to the intruder can access system normally with disguise, Circuit Patrol model has been suggested to monitor from intrusion attack.

* 동원대학 e-비즈니스과 교수

논문접수 : 2002. 3. 29
심사완료 : 2002. 6. 1

Ⅰ. 서론

초고속 정보통신망의 확대는 관, 산, 학, 연은 물론 일반일들도 인터넷을 이용하여 전 세계의 서버에 접속을 할 수 있게되었다. 유선 인터넷의 급성장에 따라 정보이용은 이제 까지 다른 매체를 이용할 때와는 완전히 다른 양상을 띄고 있다. 이는 인터넷 역할이 규모나 활용 측면에서 양적·질적 차원으로 사회 각 분야에서 파급되어 활성화되고 있기 때문이다. 이에 따라 정보검색, 정보서비스를 통한 정보 공유와 전자상거래, 전자서명, 전자결제 등을 통한 전자거래가 대중화되어 가고 있다.

이러한 추세는 전 세계인이 정보를 신속히 찾아서 실생활 및 업무에 활용할 수 있다는 유용한 면이 있다. 하지만, 서버에 보관되어 있는 개인정보, 기업비밀, 군사비밀, 그리고 국가비밀 등을 빼내어 악의적으로 사용하는 경우도 증가되고 있는 추세이다. 그러므로, 국가기관, 산업체, 대학, 연구소 등은 인가되지 않은 사용자가 시스템에 침입하게 되어 파괴, 절취 등의 손상을 입게 되었다. 즉, 시스템 침입자는 데이터 삭제, 데이터 이동, 시스템 파괴 등 파괴 행위와 정보유출 등의 도용을 하여 도적적, 경제적 등의 손실을 입히고 있는 실정이다. 침입탐지 시스템에 대한 연구는 주로 시스템 접근방지를 위한 탐지 시스템 측면에서 많이 진행되어 왔다.

이러한 유선 인터넷의 추세는 모바일 폰의 확산으로 인하여 점차적으로 무선 인터넷으로 전이되어 가고 있다. 모바일 폰의 확산은 모든 사람들에게 유선 인터넷에서 충족을 못시켰던 점 들 중 휴대성과 이동성을 약속해 주었기 때문에 무선 인터넷이 증가하고 있는 추세이다. 이로 인하여, 기업의 일선(front line)에서 근무하는 업무 담당자들은 지역에 관계없이 이동을 하면서 기업정보에 즉시 접근할 수 있게 되었다. 또한, 일반인들도 모바일 폰, PDA를 실생활에서 이용하게 됨에 따라 기업정보의 도용은 물론 개인정보를 악용하는 경우가 자주 등장함에 따라 정보보호가 사회전반에 큰 이슈화되고 있다. 모바일 폰의 증가에 따른 정보침입이 예견됨에 따라, 모바일 폰을 통한 시스템 내부의 정보침입을 탐지하고 대응할 수 있는 시스템이 요구되고 있다.

또한, 방화벽은 시스템 내부와 시스템 외부인 인터넷상의 접속점간 데이터의 통과를 감시, 차단하는 시스템이다. 이에 따라, 시스템 내부를 방화벽으로 보호하여 FTP(File Transfer Protocol) 등의 명령은 거부하나, 시스템 외부에서 시스템 내부로 들어오는 전자메일 등의 데이터 등은 차단할 수 없는 문제점이 있다. 보안이 철저히 요구되는 시스템에는 보다 한 차원 높은 보안을 고려하여 패스워드를 엄격히 고려하고 있으므로 본 논문에서 원타임 패스워드에 의한 트랩을 설치하여 침입여부의 대한 파악 및 추적을 하고자 한다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 유선 인터넷의 침입 유형과 침입탐지 기법을 살펴본 후 침입탐지 기법에 대하여 살펴보고, 3장에서는 무선 인터넷에서의 침입유형을 살펴보고, 4장에서는 모바일 폰을 통한 시스템 침입으로부터 정보보호를 위한 침입탐지 시스템을 설계하고자, Circuit Patrol을 이용한 침입탐지에 대한 설명 및 모델에 대한 설명을 하고자 한다. 5장에서는 결론 및 향후 연구 과제에 대하여 설명하고자 한다.

Ⅱ. 유선 인터넷의 침입 유형과 침입탐지 기법

침입은 컴퓨터 시스템에서 이용되는 자원의 무결성(Integrity), 비밀성(Confidentiality), 가용성(Availability)을 저해하는 행위로서 비정상적(anomalous) 침입과 오용(misuse) 침입으로 분류해 볼 수 있다[3]. 침입탐지는 컴퓨터 시스템이 크래킹 등 해킹 공격에 사전대비 및 사후대응을 하는 행위이다. 이를 위하여 시스템 자원과 네트웍 자원에 대한 비정상적인 사용이나 오용 등에 대한 정보를 지속적으로 수집하고 분석하여 침입탐지를 감시하는 시스템이다.

2.1 침입유형

비정상적(anomalous) 침입은 컴퓨터 시스템 자원에 대한 비정상적인 행위 또는 사용을 위한 침입이다. 이에

반하여, 오용(misuse) 침입은 컴퓨터 시스템 또는 소프트웨어의 결점을 통하여 컴퓨터 시스템 자원에 침입하는 해킹 공격을 말한다[5].

2.2 침입탐지 기법

침입탐지 시스템은 엔진유형, 실시간 분석, 그리고 검사 데이터 종류 등에 의하여 분류되기도 하는데[5], 침입탐지 시스템은 크게 호스트 기반의 침입탐지 시스템, 유·무선 네트워크 기반의 침입 탐지 시스템 등으로 나누어 볼 수 있다. 호스트를 기반으로 한 침입 시스템은 감사로그 정보를 이용하여 컴퓨터 시스템 상에서 발생되는 이상징후의 정보를 감시한다. 유선 네트워크를 기반으로 한 침입 시스템은 유·무선 네트워크 상에서 전송되는 패킷과 프로토콜을 분석하여 이상징후의 정보를 감시한다.

비정상적 침입에 대한 침입탐지 기법에는 비정상 측정(anomaly measures), 신경 네트워크(neural network), 예측패턴 생성(predictive pattern generation), 통계적 접근(statistical approaches), 특징 추출(feature selection) 등이 있다[5].

오용 침입에 대한 침입탐지 기법에는 모델 기반의 침입탐지(model based intrusion detection), 상태 전이 분석(state transition analysis), 전문가 시스템(expert system), 조건부 확률(conditional probability), 키 타격 모니터링(keystroke monitoring)[5].

비 정상측정기법은 정상적이지 않은 행동들을 탐지하는 기법이다. 신경 네트워크 침입탐지 기법은 뒤 따라 일어날 명령을 신경 네트워크 학습방법을 통하여 사전 예측하는 기법이다. 이 탐지기법은 뒤 따라 일어날 명령어가 예측된 명령이 아닐 때 비정상적인 접근을 탐지하는 기법이다. 예측패턴 생성 침입탐지 기법은 발생할 사건의 순서는 예측할 수 있는 패턴이 있다는 가설에 따른다. 이 탐지기법은 사건간의 상호관계와 순서에 따라 발생한 사건의 비정상적인 접근을 탐지하는 기법이다.

통계적 접근 침입탐지 기법은 과거의 자료를 통계적으로 처리한 침입탐지 기법이다. 측정하여 사용하는 과거의 자료들로는 활동밀도, 파일접근 확률분포, 입·출력 확률분포, 로그인 횟수, CPU 또는 입·출력 사용 양 등이다. 이 탐지기법은 프로세스 행위에 대한 프로파일을 생성한 다음, 프로파일의 비정상적인 프로세스를 관찰하는 기법이다.

특징 추출 침입탐지 기법은 특징이 있는 침입패턴을 추출하는 침입탐지 기법이다. 측정방법으로는 베이지안 통계량, 공분산 매트릭스 등이 있다. 이 탐지기법은 알려진 침입탐지 측정도구들을 설정하여 놓고, 이중에서 침입을 예측하거나 분류할 수 있는 침입탐지 도구들을 선택하여 침입을 탐지한다.

모델 기반의 침입탐지 기법은 증거를 바탕으로 한 추론을 이용하여 침입을 탐지하는 기법이다. 이 탐지기법은 침입패턴들을 데이터베이스화 한 다음, 침입이 발생할 경우 데이터베이스를 참조하여 침입을 탐지한다.

상태 전이 분석 침입탐지 기법은 시스템 상태전이 순서를 참조하여 침입을 탐지하는 기법이다. 이 탐지기법은 침입패턴들을 시스템 상태전이 순서로 표현한 한 다음, 침입이 발생할 경우 이 패턴들을 참조하여 침입을 탐지한다.

전문가 시스템 침입탐지 기법은 침입패턴에 대한 지식규칙을 이용하여 침입을 탐지하는 기법이다. 즉, 과거의 침입패턴에 대한 지식규칙을 구축한 후, 감사추적 사건과 일치되는 사실들을 명시한다. 침입이 발생할 경우에는 이 지식규칙과 사실들을 참조하여 침입을 탐지한다.

조건부 확률 침입탐지 기법은 침입이라고 단정할 수 있는 판단을 조건부 확률을 이용하여 특정 이벤트가 발생할 침입을 탐지하는 기법이다.

키 타격 모니터링 침입탐지 기법은 사용자의 키 타격을 모니터링하여 침입공격 패턴 발생을 결정하여 침입을 탐지하는 기법이다.

그러나, 기존의 침입탐지 시스템에서는 침입행위가 일어난 후 탐지를 하기 때문의 시스템 자원이 이미 누출되고 손상된다는 점이 문제점이므로 능동적인 추적기능을 추가하여 보안사고 방지가 필요로 하다[2]

Ⅲ. 무선 인터넷의 침입 유형

모바일 폰의 대중화에 따라 개인들의 정보이용 급증은 물론, 기업의 업무용으로도 그 용도가 확대되어 가고 있다. 이에 따라 사용자의 번호 도용과 불법 사용으로 인하여 정상적인 사용자에게 과금, 통화정보의 도청 등의 큰 손실을 입히고 있다[4]. 무선 인터넷 통신환경과 관련된 보안

서비스에는 인증(Authentification), 암호(Encryption), 당사자 익명성(Party anonymity), 키 관리(Key Management) 등이 있으며, 모바일 폰 사용자들은 도메인의 인증 서버를 통하여 상대방간 인증 되는데, 이를 위하여 비대칭 암호와 대칭 암호기법을 사용한다.

네트워크 내의 인증센터, 기지국의 조작으로 특정 단말기 사용자의 위치를 추적하여 개인 사생활 정보에 대한 침해가 일어 날 수도 있다[8]. 또한, 무선 인터넷에 연결된 상태에서의 데이터 전송시에 통신 중 통화권 이탈과 상대방의 강제에 의한 접속 단절, 오류 등으로 인하여 데이터베이스의 일관성에 위협을 가하기도 하는데, 이러한 연결의 단속은 결국 해커들의 무선 단말기나 기지국에 공격을 할 수 있는 기회를 주기도 한다[7].

신분 가장에 의한 데이터 공개, 데이터 도용 등도 공증과 정보의 접근으로 인하여 발생될 수가 있기 때문에 무선 인터넷의 사용으로 정보 도청이 용이해 질 수 있다[4].

Ⅳ. Circuit Patrol을 이용한 침입탐지 모델

4.1 WML 기반의 WAP 구조

무선 인터넷 서비스를 위한 WAP(Wireless Application Protocol)의 구조는 〈그림 1〉과 같다. 즉, 클라이언트, 서버, 그리고 게이트 등의 구조로 이루어져 있다. 클라이언트 부분은 휴대폰 단말기, PDA 등이고, 서버 부분은 웹서버, 데이터베이스 서버 등이다. 게이트웨이(Gateway)는 클라이언트와는 무선네트워크로 연결되며, 서버와는 유선 네트워크로 연결된다.

무선 인터넷 서비스는 클라이언트 요청에 따라 서버가 응답을 하는 풀(Pull) 방식과 서버가 클라이언트에게 전달하는 푸시(Push) 방식으로 나누어 볼 수 있다. 클라이언트인 모바일 폰은 WAP 게이트웨이를 통하여 입력된 URL에 위치한 웹 서버로 부터 데이터를 요청한다. 그러면, 요청된 URL에 위치하고 있는 웹 서버는 WAP 게이트웨이를 통하여 클라이언트인 모바일 폰에게 정보를 전달한다.

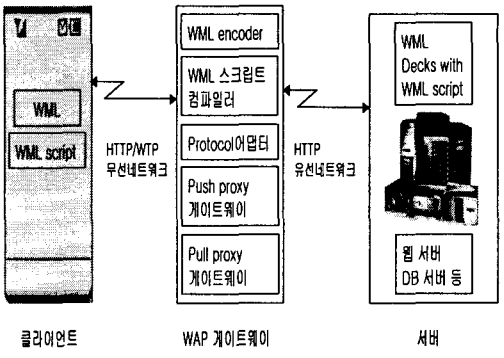

그림 1. WML 기반의 WAP 구조

4.2 RIAS 모델의 기본구조

아래의 그림은 알려진 침입 기법들을 탐지하여 모바일로 그 침입사항을 알려주는 원격 침입 경보 시스템(RIAS: A Remote Intrusion Alert System)으로서 그 구조는 감사자료 수집모듈, 침입탐지 모듈, 침입기법 분류모듈 등으로 되어 있다[1].

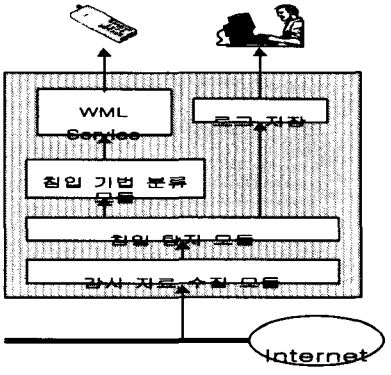

그림 2. RIAS 모델의 기본구조[1]

감사 자료 수집 모듈에서는 이더넷 프레임부터 TCP 세그먼트까지 상세한 정보를 얻을 수 있는 필터링 방법을 이용하여 자료를 수집하였으며[9], 침입 탐지 모듈은 수집된 네트워크 패킷을 이용하여 Smurf Attack, Land Attack, Network Scan, SYN flooding, Buffer Overflow 등의 침입기법을 탐지하게 된다[1].

4.3 Circuit Patrol을 이용한 침입탐지 설계

기존에 제안된 대부분의 침입 탐지 시스템들은 유선 인터넷을 통한 시스템 접근에 대한 침입을 탐지하는 시스템이었다. 또한, 하나의 통합된 단일 시스템 구조를 가지

고 있어 탐지 모듈의 파괴에 다른 안전성 문제, 시스템 확장에 따른 성능보장에 한계점이 있었다.

본 논문에서 제안한 모델은 무선 인터넷을 통한 침입에 대한 탐지를 위한 시스템에 적용될 수 있으면서, 기존 유선 인터넷과 연결된 시스템에서도 적용할 수 있는 침입탐지 모델을 제시하였다. 이에 따라, 원타임 패스워드 방식에 의하여 호스트 또는 시스템에 접속한 흐름을 체크하여 이를 분기하고 원타임 패스워드 규칙에 위반한 접속은 별도의 트랩으로 유도하여 침입인 경우에는 탐지, 경보, 보고를 하는 모듈로 구성하였다. 원타임 패스워드 규칙을 통과한 접속이라고 하더라도 각 데이터 폴더 클러스터링에는 Circuit Patrol이 접속 패킷에 대한 모니터링을 통하여 데이터의 손상, 멸실, 오용 등을 방지하도록 설계하였다.

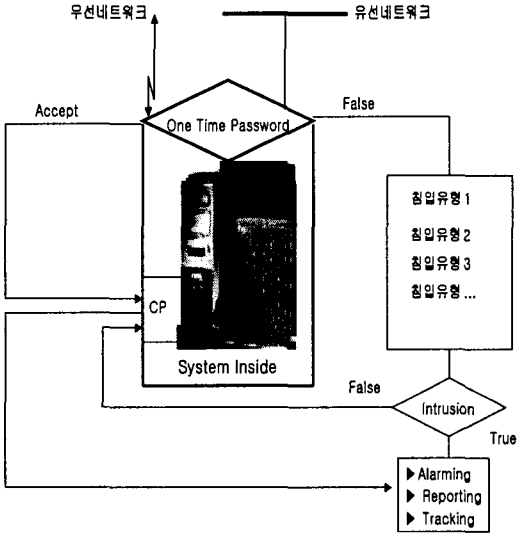

그림 3. 제안된 CP 침입탐지 구조

■ 설계 시 고려사항

원타임 패스워드, 트랩, CP(Circuit Patrol), 침입탐지 체크범위, 그리고 경고 및 보고 등에 대한 설계시 고려사항은 다음과 같다.

(1) 원타임 패스워드

크래커들은 텔넷 등의 원격 로그인을 통하여 침입을 목표로 하는 시스템에 접근을 하는데, 이때 대부분 패스워드에 의하여 시스템 접근에 대한 허용을 받는다. 패스워드는 허용된 사용자를 확인할 수 있는 부분으로서 시스템 내부에는 ID와 패스워드에 대한 암호화된 패스워드 데이터베이스를 작성해 놓고 시스템을 사용하려고 하는 자가 패스워드를 입력시 이를 비교하여 허가여부를 판단한다. 그러나, 시스템 관리자의 권한을 취득하면 패스워드 데이터베이스 접근이 가능하여 무용지물이 되고 만다. 따라서, 이를 보완하기 위하여 원타임 패스워드 방식이 소개되었다. 원타임 패스워드는 외부에서 시스템에 접근시 사용을 하였던 패스워드는 다시 사용할 수 없도록 한 패스워드로서, HHA(Hand Held Authentificator)를 사용하여 생성된 코드를 이용하여 원타임 패스워드를 작성하는 Challenge Response와 사용자 각자에게 부여되는 고유의 비밀 데이터인 패스 플래이즈와 패스워드 생성 프로그램을 사용하여 원타임 패스워드를 작성하는 S/Key 방식이 있다[10]. 원타임 패스워드에 부합하지 않으면, 우선 비정상 사용자로 보고 시스템 내부의 별도장소인 트랩으로 옮긴 후, 알려진 침입탐지 기법을 적용한다.

(2) 트랩

원타임 패스워드 규칙에 위반한 접속인 경우에는 우선, 침입 가능으로 간주하고 관련된 침입공격 유형 등과 비교하여 감시한다. 만일 침입으로 간주되지 않으면, 정상 접속자로 보고 시스템 내의 CP로 연결을 하며, 그 후 정상을 가장한 침입여부를 지속적으로 감시한다.

(3) CP(Circuit Patrol)

CP는 시스템 내부의 데이터 클러스터링 헤더에 설치된 패트롤로써 에이전트 기능으로 볼 수 있다. 이 CP의 상위에는 CPM(Circuit Patrol Manager)이 전체 시스템내에 중요 데이터 클러스터링 헤더에 위치하고 있는 CP들을 관리한다. 즉, CPM은 CP들이 보고하는 침입여부를 보고 받고 경보를 시스템에 전달하며, 그리고 침입자를 추적하는 역할을 한다.

CP(Circuit Patrol)에서는 원타임 패스워드를 통과하여 들어온 자들의 행동을 추적하고 그 행동을 비교하는 역할을 한다. 기존 정상적인 사용자들의 시스템 내부에서의 업무수행 행동 흐름은 ID 별로 데이터베이스(Behavior DB)화 한다. 패트롤에서는 접속을 요청하는 시스템 외부자의 행동을 주시하며, 시스템 외부에서 들어온 자의 행동을 TCP/IP의 헤더를 읽어 시스템 접근 처음부터 목적지와 소스, 그리고 행동을 추적하며 기록한다. 기존의 행동 패턴과 비교하기 위하여 데이터 접속시간, 중복여부, 접근여부, 파일손상 여부 등을 모니터링 하

여 허용범위 및 권한 범위를 넘어서는 지를 지속적으로 감시한다. 그리고, Behavior DB와 비교하여 매칭이 안될 경우에는 침입으로 간주하고 경고를 한다.

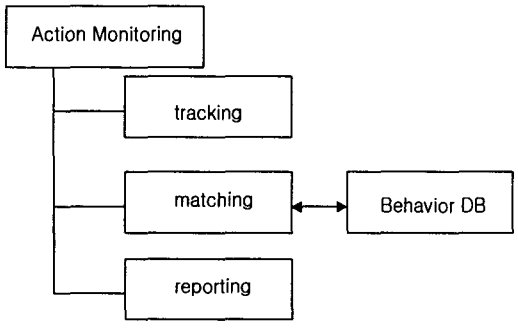

그림 4. CP 구조

(4) 침입탐지 체크범위

침입탐지를 체크할 범위는 호스트 기반과 WAN 등의 유선 네트워크기반에서 비정상 행위와 오용 등을 위하여 침입하던 기존의 공격(Smurf Attack, Land Attack, Network Scan, SYN flooding, Buffer Overflow 등)과 무선인터넷을 통한 침입유형 등에 대한 모든 행위가 탐지되어야 한다.

(5) 경고 및 보고

침입으로 판단되면 관리자에게 불법침입에 대한 경보 전달과 더불어 보고체계에 따라 사후관리를 한다. 또한, 침입경로의 추적과 더불어 실시간으로 침입자를 감시하고 추적할 수 있어야 한다. 그리고, 불법 침입으로 판정되었을 때는 더 이상 시스템에 접근하지 못하도록 네트워크 패킷을 제거, 또는 로그 아웃 등의 방법을 사용해서 차단할 수 있어야한다.

V. 결론 및 향후 연구 과제

최근, 휴대폰, PDA 등 모바일 기기들을 활용한 업무가 개인부터 기업, 관공서에까지 확대되고 있는 추세이다. 이에 따라, 본 논문에서는 정보보호를 위한 침입탐지 시스템을 설계하고자, 유선 인터넷의 침입 유형과 침입탐지 기법을 살펴보았다. 그리고 무선 인터넷에서의 침입유형을 살펴본 후 침입에 대한 침입탐지를 위하여 circuit patrol을 시스템 내부에 위치시켜 모바일을 통한 내부침입에 대한 공격을 탐지하는 모델을 제시하였다.

본 논문의 향후 연구과제는 인공지능을 갖춘 CP 시스템을 설계하고 구현하고자 한다. 이를 위하여 데이터 클러스터링에 대한 학습시스템을 실제 시스템내에서 구현하는 추가적인 연구가 수행되어야 할 것으로 본다.

참고문헌

〈국내논문〉

[1] 강태호, 김원진, 방훈, 원대희, 이재영, "WAP 기반의 침입기법 차별을 이용한 원격침입 경보시스템", 정보과학회 춘계학술대회, 2002

[2] 신도경, 이종성, 채수환, "NetRanger 시스템의 침입탐지 기능 향상 및 추적 환경에 관한 연구",

[3] 심영철, 장영민, 변경근, "온라인 네트워크 침입탐지 및 감시 도구", 과학기술 연구논문집, Vol.8, No.1, 1997

[4] 이상철, 이충호, 오영환, 임기욱, 배해영, "모바일 지리정보시스템에서 보안을 고려한 설계", 한국정보처리학회 춘계학술발표논문집 제8권 제1호, 2001, pp.81-84

[5] 차현철, 권용철, "패킷 패턴 테이블을 이용한 침입탐지 시스템 모델", 동양대학교 산업기술연구소 논문집 Vol.3 No.1, 2001

[6] 차현철,"삽입 및 배제 공격을 고려한 네트워크 침입탐지 시스템 모델", 한국 OA논문 학회지 제5권 제4호, pp.69-75. 2000.12.

〈외국문헌〉

[7] Astrid Lubinski, "Security Issues in Mobile Database Access", KLUWER ACADEMIC PUBLISHERS, 1999

[8] Artem Garmash, "A Geographic XML based Format for the Mobile Environment", Proceedings of the 34 Hawaii International Conference on System Science, 2001.
[9] Steven McCanne, Van Jacobson, "The BSD Packet Filter: A new Architecture for User level Packet Capture", Dec. 19,1992.
[10] Suart Mcclure, Joel Scambray, George Kurtz, "Hacking Exposed Network Security, Secrets & Solutions", 3rd. ed.

저 자 소 개

장 덕 성
서울 산업대학교 산업공학과(학사)
고려대학교 경영정보 전공(석사)
경원대학교 경영정보 전공(박사)
서울보건대학 사무자동화과 겸임교수
남서울 대학교 전자계산학과 겸임 교수
현재, 동원대학 e-비즈니스과 교수
관심분야: e-비즈니스, 모바일