제한된 내부 네트워크 정보 접근제어와 계층별 클라이언트 권한설정 관리에 관한 연구

서우석* · 박재표** · 전문석***

A Study on Control of Access to Internal Network Information and Authority Set Up Management for Client by Class

Woo-Seok Seo* · Jae-Pyo Park** · Moon-Seog Jun***

요 약

정보처리 시스템의 프로세서가 작업 대상으로 하는 다양한 콘텐츠 정보가 온라인상에서 놀라울 정도로 확대되어진 시점은 불과 몇 년 전이다. 2000년을 실시간 공유와 같은 정보 및 자료의 홍수가 이루어진 기술기반의 해라면, 이후 2011년까지는 활용기반의 기능과 솔루션이 넘쳐나는 기간이었다. 또한 이러한 정보처리 시스템의 활용도가 높아지는 과정 속에서 2009년과 2010년에는 대규모 개인정보의 유출사건이 발생한바 있고 정보의 보호를 위한 방어와 보호를 위한 기술과 솔루션들이 지속적으로 개발, 적용되고 있다. 하지만 외부로부터의 불법접근의 문제점에서 그 범주가 확대되어 내부 사용자 또는 내부 정보처리 시스템과 클라이언트 시스템에 숨겨진 Agent 등으로 인한 피해는 날로 증가하고 있다. 따라서 본 논문에서는 내부정보에 대한 접근제어와 관리자 및 내부 사용자의 계층별 권한설정에 대한 효율성 기반의 정보보호를 위한 연구가 필요하며, 본 연구 결과로 SOHO급 네트워크에서 대규모 네트워크에 이르기까지 실무에서 보안기법으로 활용 가능한 연구 자료를 제공코자 한다.

ABSTRACT

It has been only few years that various contents information subject for information processing system has been remarkably increased in online. If we say the year 2000 is the technology based year when deluge of information and data such as real time sharing, the time since after 2000 until 2011 has been a period plentiful of application based functions and solutions. Also, as the applicable range of these information process systems extends, individual information effluence has been social issues twice in 2009 and 2010. Thus now there are continuous efforts made to develop technologies to secure and protect information. However, the range problem has been extended from the illegal access from outside to the legal access from internal user and damages by agents hidden in internal information process system and client system. Therefore, this study discusses the necessity for the studies on efficiency based information security by control of access to internal information and authority setting for administrator and internal users. Based on the result of this study, it provides data that can be used from SOHO class network to large scale for information security method.

키워드

Information Security, Internal Network Information, Control of Access, Authority
정보보호, 내부 네트워크 정보, 접근제어, 계층별 권한

* 숭실대학교 일반대학원 컴퓨터학과(ssws2003@yahoo.co.kr) ** 교신저자 : 숭실대학교 교수(pjerry@ssu.ac.kr)
접수일자 : 2012. 01. 03 심사(수정)일자 : 2012. 03. 15 게재확정일자 : 2012. 04. 07

Ⅰ. 서 론

정보보안을 위한 방어기법은 과거 특정 영역에 대한 1차원적인 기술과 기능으로 접근을 제어하는 등의 방법으로 보안을 유지했다. 하지만 외부로부터 불법적인 접근을 시도하는 경우에 대한 방법 또한 다양화되고 그 기술의 진보가 빠르게 진척됨으로 인한 다차원의 방어기법이 필요하게 되었다.

물론 다차원의 방어기법이 개발되고 실용화되는 계기로는 2009년 온라인상에서 인터넷 대란, 2010년 금융권 개인정보 등 유출, 2011년 계속된 정보 침해사건 등으로 인해 많은 보안기술 개발 업체와 관련 기기 판매업체들이 더욱 빠르게 시장에 정보보안 기기와 솔루션을 제공하기 시작하면서 이루어지고 있다.

정보에 대한 불법적인 접근 형태와 방법은 외부와 내부로 이원화하여, 그 범주를 구성할 수 있으며, 각 범주에 따른 침해 비율은 외부가 내부 접근에 비해 다소 높은 편이다.

또한 외부 침입에 대한 부분만을 방어의 범주로 제한하고 특정 네트워크에 대한 방어만을 위한 특화된 기술이 주로 개발되고 구현되어왔으나, 다차원의 방어기법에서는 내부로부터의 불법 접근에 대한 시각과 견해가 새롭게 인지하는 부분에 중점을 두고 기술개발이 이루어지기 시작했다[1].

따라서 본 논문에서는 제한된 내부 네트워크 정보 접근제어, 계층별 클라이언트 권한설정에 대한 방법을 제안하고 검증함으로써 결과를 도출하고 정보처리 시스템으로부터 산출된 산출물에 대한 안전한 접근관리와 활용권한에 대한 연구를 한다.

Ⅱ. 관련연구

본 논문에서는 기존의 정보처리 시스템의 활용방법을 변형함으로써 시스템내의 정보에 대한 접근에 있어서 접근제어 형태와 권한설정 관리 부문에 대한 형태를 제안하고 기존에 운영했던 다양하게 흩어져 있는 접근제어와 권한설정 관리 기술들을 집약하고 계층화 분리함으로써 정보처리 시스템이 생성하고 저장하는 정보와 자료에 대한 안전성을 확보하는데, 그 의의가 있다[2][3].

따라서 정보보호를 위한 현장(실무)에서 관리자뿐만 아니라 일반 사용자에게 이르기까지 다양하고 안정적인 보안을 위한 매뉴얼인 지침과 같은 가이드라인을 제공하고자 한다.

또한 관련연구에서는 접근제어와 권한설정 관리 기술의 객관성과 기존 기능과 솔루션과 비교를 위한 적절한 침해사례 분석과 정보보호 구현 제반환경, 정보처리 시스템이 생성하고 운영하는 데이터베이스의 종류 등을 확인하고 기존 접근제어와 권한설정 관리에 대한 기초자료를 확인한다.

2.1 침해 솔루션 기반의 침해신고 현황

다양한 침해사고 현황을 보면, 외부로부터의 접근에 대한 방어 기술만이 편중된 개발이 이루어지고 있음을 알 수 있다. 하지만 다차원의 방어기법에 대한 연구와 개발이 이루어지면서 정보유출로 인한 파급되는 문제점, 장애비율 등과 같은 내부에서 발생하는 부분 또한 상당히 높은 침해비율이 발생하고 있음 또한 인지하고 있다.[4].

표 1은 최근 6개월간에 발생한 내부 시스템 또는 네트워크에 잠복함으로써 능동적이고 자립적인 판단에 따른 처리기능을 갖는 함수 또는 침해 솔루션에 의한 정보 유출과 시스템 장애를 유발시키는 불법적인 침해 솔루션 기반(Agent) 침해신고 비율이며, 향후 접근제어와 권한설정 관리에 대한 기법제안 과 검증을 위한 기초자료로 활용할 것이다[5].

표 1. 2011년 침해 솔루션 기반(Agent) 침해신고 비율
Table 1. Report rate of Infringement by Infringement Solution Agent

구분	명칭	건수	월별변동 비율	분기별 변동비율
3월	침해 솔루션 기반 (Agent)	192	-	-
4월		220	12%	-
5월		206	▲7%	7%
6월		165	▲25%	-
7월		211	21%	-
8월		222	5%	26%

* 월별변동과 분기별 변동비율은 참고문헌 자료 내에서 산출 계산한 비율임

**** 표-1의 침해신고 비율 산출 예제***

- 3월 대비 4월 불법적 침해 솔루션 기반(Agent)

*상승 비율 : ((192/220)-1)*100=13%*
- *3월 대비 5월 불법적 침해 솔루션 기반(Agent) 상승 비율 : ((192/206)-1)*100=7%*
- *3월 대비 6월 불법적 침해 솔루션 기반(Agent) 상승 비율 : ((192/165)-1)*100=▲16%*
- *3월 대비 7월 불법적 침해 솔루션 기반(Agent) 상승 비율 : ((192/211)-1)*100=10%*
- *3월 대비 8월 불법적 침해 솔루션 기반(Agent) 상승 비율 : ((192/222)-1)*100=13%*

2.2 접근제어 및 권한설정 관리 운영현황

정보처리 시스템을 이용함으로써 생성되고 최종 산출되는 결과물은 다양한 데이터베이스에 의해 보존되고 저장되어 재활용 된다. 따라서 각 시스템마다 운영하는 DBMS(DataBase Management System) 현황 확인을 그림 1과 같이 실제 예처럼 확인하고 접근을 제어하고 각 사용자에 대한 권한설정 관리를 위한 툴에 대한 활용정보를 실제 다룰 줄 알아야 한다.

그림 1. 정보처리 시스템 활용 데이터베이스(예> Microsoft SQL Server) 관리자 모니터링
Fig. 1 Database administrator monitoring by information process system (e.g. Microsoft SQL server)

또한 표 2와 같이 데이터베이스 종류, 운영환경, 데이터베이스 암호화(특정 데이터베이스뿐만 아니라 정보를 암호화 가능한 모든 솔루션을 제시) 종류에 대한 현황을 확인함으로써 각 정보처리 시스템에 대한 사용 및 접근 권한관리와 제어가 가능해 진다[6][7][8].

표 2. 정보처리 시스템이 생성하고 운영하는 데이터베이스 및 암호화 솔루션 현황
Table 2. Current status of database and password solution administered by information process system

구분	내용		
DB 종류	Oracle	MySQL	Informix
DB 내역	Unix 환경 / RDBMS	Unix, Linux, Windows 환경 / RDBMS	Unix 환경 / RDBMS
암호화 종류	- Data Encryption Standard [비밀 키 방식의 일종으로 64비트의 키를 사용하여 64비트의 평문을 전자(轉字)와 환자(換字)를 조합하여 암호화하는 방식] - Public Key Infrastructure [공개 키 암호 시스템을 안전하게 사용하고 관리하기 위한 정보보호 표준 방식] - Privacy Enhanced Mail [비밀성, 메시지 무결성, 사용자 인증, 발신자 부인 방지, 수신자 부인 방지, 메시지 반복 공격 방지 등의 기능을 지원] - Rivest Shamir Adleman [암호화 알고리듬을 사용하는 공개 키 암호 방식] - Pretty Good Privacy [메시지의 내용을 암호화 알고리듬을 사용하여 암호화] - Public Key Cryptography Standards [안전한 정보를 교환할 수 있도록 산업계에서 사용되는 일련의 공개 키 기반 표준 프로토콜]		

III. 내부 정보보호를 위한 접근제어 및 권한설정 관리 기법

접근제어와 권한설정 관리는 다양한 데이터베이스 중에 선정하여, 운영하는 데이터베이스 또는 정조처리 시스템 상에서 제공하는 서비스를 이용하기 위한 총괄 관리권한자와 일반 접근 사용자에 대한 각각의 보안 등급을 구분하고 각 등급에 맞는 접근 제한 등의 솔루션을 적용함에 있어 개발사마다 일괄성이 없다. 즉, 개발사에 따라 보안 등급선정을 위한 기준 지표와 등급 조정에 대한 솔루션 기본정보가 상이함을 의미한다.

따라서 종합적인 정보보안을 위한 융합 관리 시스템 재개발은 기존의 정보 구성 매체인 데이터베이스 형태를 유지하면서 개발해야 하기 때문에 Customizing을 통한 접근이 가장 적절하다.

Customizing을 통한 내부에 존재하는 정보에 대한 보안을 위한 접근제어와 권한설정 관리를 위한 기법을 제시하기 위해서는 첫 번째. 정보처리 시스템 권한 영역 제한과 두 번째. 산출 및 도출과 생성 정보 접근 방식 이원화, 세 번째. 온라인 정보와 오프라인 정보 처리 프로세서 연계 등 세 가지 확인 자료에 대한 근

거가 요구된다.

3.1 정보처리 시스템 권한설정 영역 제한

각각의 다양한 Plat-Form으로 구성된 데이터베이스를 가지고 정보처리를 목적으로 하는 시스템이 지원하는 권한관리 기본 설정과 제반환경을 그림 2와 같이 Information Processing System[이하 ISP라 한다]가 존재하는 고유한 영역으로 범주를 제한하고 나눔으로써 생성되고 보존중인 데이터베이스 정보에 대한 구성과 종류에 대한 최초 생성 경로를 확보한다.

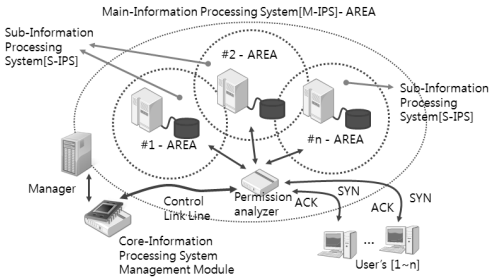

그림 2. 권한설정 관리 영역과 영역별 적용 프로세서 현황
Fig. 2 Current status of authority setting and administration domain and the applied processor to each domain

따라서 정보에 대한 각 소스에 해당되는 데이터베이스의 영역을 구분하고 원래의 정보가 역으로 최초 생성하고 보존중인 정보처리 시스템으로의 회귀 가능한 정보를 기본적인 정보구성 형태로 형성시킨다.

또한 제한된 내부 네트워크 영역과 정보처리 시스템 영역을 융합함으로써 특정한 임시의 영역으로 구성하고 Permission Analyzer[이하 PA라 한다] 및 Core-Information Processing System Management Module[이하 C-IPSM2라 한다]을 이용해서 전체 권한설정 관리 영역과 영역별 적용 프로세서 운영과 관리를 조정하고 실제 소프트웨어적인 관리를 시행한다.

* *Main-Information Processing System[M-IPS]*
- *Sub-Information Processing System별 영역을 일괄 하나의 영역으로 구성한 총괄 영역 관리 시스템*

* *Sub-Information Processing System(#1~#n)[S-IPS]*
- *목적과 산출물에 상관없이 정보가 생성 가능한 시스템을 대상으로 유사 데이터베이스를 구축하고 집약하는 영역별 관리 시스템*

* *Permission Analyzer[PA]*
- *각 IPS에 접근하는 관리자 및 사용자들에 대한 정보처리 시스템 산출물인 데이터베이스 접근 권한 설정의 한계를 확인하는 모듈*

* *Core-Information Processing System Management Module[C-IPSM2]*
- *전체 [Main, Sub] IPS를 관장하고 총괄 운영 및 관리하는 관리자 단의 핵심 정책 구현 모듈*

3.2 정보처리 시스템 생성 정보 접근 방식의 이원화

최근에 들어서 Virtual Machine 솔루션들과 Cloud Computing에서 많이 활용하고 있는 이원화 과정과 개념을 이용한 접근 경로를 이원화한 방식으로 2가지의 접근을 제어하는 방법을 활용한다.

우선 접근 경로를 이원화 방식이란 정보처리 시스템으로부터 최초 생성되고 프로세서에 의해 생성되고 있는 정보, 필요에 의해 인위적으로 삭제 처리되어진 정보에 대한 접근 경로를 각각 다르게 설정함에 따라 정보의 유출과 접근을 차단하는 방식을 의미하며, 그림 3은 1차적으로 접근 경로 이원화를 기반으로 원래

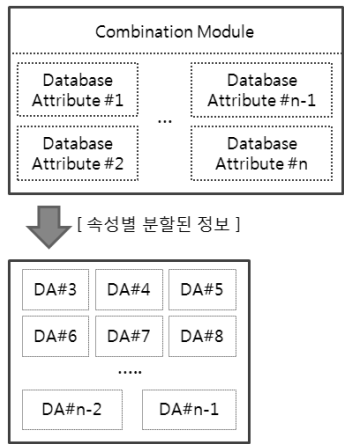

그림 3. 데이터베이스 구성 요소에 대한 구성속성별 분할과 조합
Fig. 3 The division and combination of attributes for the components of the database

의 정보 구성 요소들 중에서 임의의 Field 영역에 고유한 특정 속성을 부여하여, 차단하거나 또는 원래의 소스를 일부 특화된 정보속성을 변형함으로써 1차적

인 접근을 제어한다.

또한 2차적으로는 속성별 분할된 정보를 별도의 데이터베이스 기록장치 또는 가상으로 구현된 Virtual Machine-Database[VMD]를 구현함으로써 이원화 방법을 적용하고 운영한다.

3.3 온·오프라인 정보처리 시스템 프로세서의 연계

오프라인 정보처리 시스템은 과거 생성되어진 정보에 대해 온라인 정보로의 변화에 맞는 콘텐츠로 변형하기 위한 과정을 거친다. 이때 변경하는 과정은 아직까지도 권한관리와 접근제어에 대한 연계부문은 가장 원시적인 방법인 오프라인 페이퍼 정보를 온라인 콘텐츠로 변경하고 이를 분리·저장하는 방법이 주를 이루고 있는 추세이다.

물론 이러한 원시적인 과정에 대한 기술 역시 부족한 기관과 기업에서는 현재도 디지털 저장 매체의 용량에 대한 제약사항과 제반 주변기기의 기술이 발전하기 이전에 생성된 정보에 대해서는 페이퍼 형태로 패쇄적인 형태로 운영되곤 한다.

그림 4는 Character Recognition Module을 이용해서 문자화 가능한 솔루션들이 이용되어지고 있는 도식을 나타낸다. 하지만 이를 데이터베이스의 구성 속성에 따른 온라인 연계방식에 대한 많은 기술이 개발되어 있으나, 반영정책에 대한 세부적인 가이드라인 등에는 부족한 부분들이 존재한다.

* *Character Recognition Module[CRM]*
- *오프라인 상에서 발생한 정보를 "Char"로 인식하고 이를 온라인 콘텐츠로 변경하고 데이터베이스 속성에 맡게 변형함으로써 온라인 정보로 활용 가능하도록 하는 모듈*

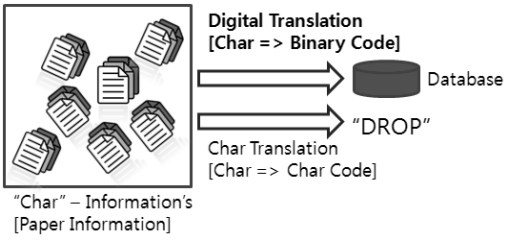

그림 4. Character recognition module 구성도
Fig. 4 Character recognition module structure chart

Ⅳ. 분산 접근제어와 중앙 집중화 권한설정 관리 기법 제안

본 논문에서 제안하고 연구하고자 하는 부분에 대한 객관적이고 투명한 결과를 얻기 위한 방법으로 앞서 서론과 관련연구에서 다양한 침해사례, 침해사고 건수, Information Processing System(#1~#n)[IPS], Permission Analyzer[PA], Core-Information Processing System Management Module[C-IPSM2], Character Recognition Module 등에 대해 논하였다.

이러한 일련의 순차적인 제시방법론은 특정한 내부 네트워크 내에 존재하는 정보에 대해 접근제어와 권한설정 관리를 위해 본 논문에서 제안하고 검증하려는 프로세서에 대한 기초자료를 제시하기 위한 것이며, 이러한 기술과 구현 논리를 펼치기 위한 모듈들은 최종적으로 중앙 집중화 권한설정 관리 구성과 사용자 분산 접근제어 기법을 제안하고 그 역할에 대한 상관관계를 파악하고자 하는데, 그 의의가 있다.

4.1 제안된 사용자 분산 접근제어 기법과 중앙 집중화 권한설정 관리 구성

제한된 내부 네트워크 정보 접근제어와 계층별 클라이언트 권한설정 관리를 위한 중앙 집중화된 권한설정 관리 방법은 그림 5와 같다.

Core-Information Processing System Management Module을 중심으로 하는 운영방법에 각각의 IPS에 따라 권한설정 관리와 접근영역을 분리함으로써 제안환경을 구성했다.

또한 이외의 Core-Information Processing System Management Module이 운영되는 동안 이원화된 Offline-Paper Information module, Character Recognition Module, Combination Module, Merge-DB : On and Offline Information을 추가적으로 함께 적용 및 운영하는 방식을 선택했다.

다만, 현실적으로 구현 불가능한 제한된 네트워크 환경으로 구성된 기관이나 기업이 있을 수 있으나, 기초적인 제안 자료로써 검증하고자 하는 것이며, 검증을 위한 기본 환경을 중심으로 분산 접근제어는 네 가지 지원 모듈로써 그 기능과 역할을 분배했다.

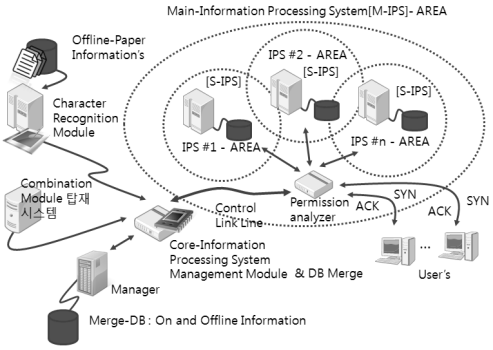

그림 5. 제안환경
Fig. 5 Suggested environment

4.2 검증 및 제안 결과와 분석

Core-Information Processing System Management Module을 중심으로 네 가지 제안 프로세서에 대한 지원 모듈을 탑재하고 이원화된 처리 모듈들을 최적의 적용이 가능하도록 구성한 제안 모델의 검증 결과가 표 3과 같다.

도출되어진 결과에 따른 한 경우를 해석해 보면, Combination Module 같은 경우에 적정 모듈 선정 운영 모듈 수로 1개를 적용하고 운영 시에 2~3%의 성능향상 비율을 나타내고 있으며, 표준오차 범위 값인 0.9~1.2%를 적용(감안)한다 해도 최종 선정 모듈 표준향상 비율은 0.9~1.9%의 성능향상 결과를 보인다. 따라서 검증에 따른 Operation Module or Active Processor 모듈의 Offline-Paper Information module을 포함한 총 5가지의 경우 모두 성능향상의 효과를 확인했다.

표 3. 적정 모듈 선정 운영 모듈 수에 따른 성능향상 비율 및 표준오차 범위와 표준향상 비율
Table 3. Optimal module selection, improvement rate of performance depending on number of operating module, range of standard deviation and standard improvement rate

Operation Module or Active Processor	적정 모듈 선정 운영 모듈 수	성능향상 비율 [%]	표준오차 범위 [%]	최종 선정 모듈 표준 향상 비율
Offline-Paper Information module	1	2~5	0.3~0.7	1.5~4.5% [0.5%]
Character Recognition Module	1	6~11	1.1~1.3	4.8~9.8% [1.2%]
Combination Module	2	2~3	0.9~1.2	0.9~1.9% [1.1%]
Merge-DB : On and Offline Information	2	3~7	1.1~1.4	1.75~5.75 % [1.25%]
Core-Information Processing System Management Module	1	24~31	6~11	15.5~22.5 % [8.5%]

* [ ] : 표준오차 범위 평균

V. 결 론

본 논문에서는 접근제어 및 권한설정 관리에 대한 검증을 통해 적정 모듈 선정 운영 모듈 수를 구하고 관련된 표준오차 범위와 이외의 변수들을 감안한 성능향상 비율과 최종 선정 모듈 표준향상 비율을 구하고자 했다.

또한 중앙 집중화된 권한설정 관리 구성과 분산 접근제어를 위해 Core-Information Processing System Management Module, Offline-Paper Information module, Character Recognition Module, Combination Module, Merge-DB : On and Offline Information이 활용되고 적용 되어 짐으로써 각 모듈의 가용 적용 수와 기능 향상 비율을 제시하고 향후 제한된 네트워크를 가진 기관과 기업에서 활용 가능한 기초자료 또는 가이드라인을 제시하고자 했다.

따라서 실험환경의 제한된 연구 영역을 확대함으로써 다양한 환경에서 실험 및 검증을 통해 향후 연구 과제로는 제안되어진 보안기법을 지속적으로 실제 환경에 적용하고 발생된 문제점을 수정하는 부분으로 개선되어야 하며, 제안하는 기법에 대한 최적화와 표준화 기반의 소프트웨어 모듈을 추가적으로 개발해야 한다.

참고 문헌

[1] 정우열, 이선근, “네트워크 환경에 적용하기 위한대칭형 혼합형 암호시스템 설계에 관한 연구”, 한국전자통신학회논문지, 2권, 3호, pp.

150-156, 2007.
[2] 엄정호, 박선호, 정태명, “내부자의 불법적 정보 유출 차단을 위한 접근통제 모델 설계”, 정보보호학회논문지, 20권, 5호, pp. 59-67, 2010.
[3] 이창훈, 하옥현, "기밀유출방지를 위한 융합보안 관리 체계", 정보·보안 논문지, 10권, 4호, pp. 61-67, 2010.
[4] 조혁현, 김정욱, 노봉남, "DSTM 터널링 보안 취약점 분석", 한국전자통신학회논문지, 2권, 4호, pp. 215-225, 2007.
[5] 인터넷침해대응센터, “인터넷 침해사고 동향 및 분석 월보”, 2011년 8월호, pp. 5, Aug, 2011.
[6] 한국정보통신기술협회, 정보통신 용어사전, http://word.tta.or.kr/terms/terms.jsp, 2005
[7] 이병엽, 박준호, 김미경, 유재수, “데이터베이스 규제 준수, 암호화, 접근제어 유형 분류에 따른 체크리스트 구현”, 한국콘텐츠학회논문지, 11권, 2호, pp. 61-68, 2011.
[8] 나성훈, 신현식, "VoIP 보안관련 주요기술에 대한 분석", 한국전자통신학회논문지, 5권, 4호, pp. 385-390, 2010.

저자 소개

서우석(Woo-Seok Seo)

2006년 숭실대학교 정보과학대학원 정보통신융합학과(공학석사)
2006년 4월~현재 서울특별시 용산구 시설관리공단 경영지원팀 전산담당
2011년 숭실대학교 일반대학원 컴퓨터학과 (박사수료)
※ 관심분야 : 정보보호, 네트워크 보안, 방화벽, Router & Network Design 등

박재표(Jae-Pyo Park)

1996년 2월 숭실대학교 컴퓨터학부 공학사
1998년 8월 숭실대학교 컴퓨터학과 공학석사
2004년 8월 숭실대학교 컴퓨터학과 공학박사
2008년 9월~2009년 8월 숭실대학교 정보미디어 기술연구소 전임연구원
2010년 3월~현재 숭실대학교 정보과학대학원 교수
※ 관심분야 : 컴퓨터통신, 보안, 암호학, 멀티미디어 통신

전문석(Moon-Seog Jun)

1981년 숭실대학교 전자계산학과 졸업
1986년 University of Maryland Computer Science 석사
1989년 University of Maryland Computer Science 박사
1986년 9월~1989년 12월 University of Mary 강사
1989년 3월~7월 Morgan State University 조교수
1989년 9월~1991년 2월 New Mexico State University Physical Science Lab. 책임연구원
1991년 3월~현재 숭실대학교 정교수
※ 관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학