프라이버시 보호 기술 및 정책에 관한 연구†

고려대학교 이유정 · 변진욱 · 이동훈

1. 서 론

정보통신망 및 컴퓨터를 이용한 개인정보의 수집 및 이용이 경제 및 사회적으로 일반화됨에 따라, 개개인의 프라이버시가 침해되는 사례가 점차 증가하고 있다. 그리고 개인들이 당하는 프라이버시 침해는 정보통신 기술이 발전할수록 더욱 더 다양해지고 지능화되고 있다. 이에 따라 몇몇 국가들은 프라이버시 침해로부터 자국민의 권익을 보호하기 위한 법률을 제정하거나 제정 중이다. 또한 세계 각국은 프라이버시 보호 관련 법제도 및 문화적 차이로 인한 원활한 정보의 유통이 저해되는 것을 방지하기 위하여 OECD 개인정보보호 8원칙 등을 반영한, 자국만이 아닌 세계적인 기준의 프라이버시 보호 기준을 마련하려고 노력하고 있는 실정이다.

국내에서도 정보화 과정의 역기능으로 나타난 프라이버시 침해 문제를 해결하기 위해 종합적인 시책을 수립하려 하지만, 현재 이와 관련된 개별법들은 각 부문별 특별법 형태로 산재해 있기 때문에 단편적이고 불균형적으로 규정된 부분이 대부분이고, 집행과 피해구제 절차의 일원화가 되지 않아 프라이버시 보호의 실효성을 확보하기는 매우 어려운 것이 현실이다. 더욱이 차세대 유비쿼터스 환경에서는 다방면에서 개개인의 프라이버시가 침해될 소지가 많기 때문에, 앞으로 제정될 법률이 실효성을 갖기 위해서는 프라이버시가 침해될 수 있는 다양한 환경이 고려되어야 한다.

이에 본 논문은 해외 프라이버시 보호 프로젝트를 중심으로 프라이버시 보호 기술의 동향을 살펴본다. 그리고 기존에 존재하던 프라이버시 보호 기술 및 프라이버시 침해 기술을 분석하고, 프라이버시 보호 기술 정책의 방향을 제시한다. 또한 현실적으로 적용 가능한 기술적 의무사항 및 조치사항들에 대해서 제시한다.

2. 프라이버시 보호 프로젝트 및 연구 동향

본 절에서는 프라이버시 보호 기술의 진행 상황 및 연구 동향을 파악하기 위해, 세계 각국에서 진행 중이거나 추진 중인 프라이버시 보호 관련 프로젝트를 살펴본다.

2.1 PORTIA

PORTIA(Privacy, Obligations, and Rights in Technologies of Information Assessment) 프로젝트는 민감한 자료들을 다루는 기술적인 기반을 발전시켜 개인정보침해 환경을 개선하는 것을 목적으로 한다[1].

2.1.1 PORTIA 주요 구성원

프로젝트의 주요 구성원은 다음 표 1과 같다. 현재 Yale 및 Standford 대학이 중심이 되어 프로젝트가 진행되고 있다.

2.1.2 PORTIA의 주제

PORTIA 프로젝트의 주된 세 가지 주제는 개인정보보호를 위한 데이터 마이닝, 데이터베이스 정책을 시행하기 위한 도구, 신원절도와 신원보호이다.

표 1 PORTIA 주요 구성원

구 분	구 성 원
주요대학 센터	Yale, Stanford
참여 대학	Stevens Institute of Technology, NYU, 뉴멕시코 대학
기술 회사	IBM, HP, Microsoft
사회단체	Citigroup, NIH, Yale Center of Medical Informatics, The Census Bureau, the Secret Service
정책 기구	CDT, EPIC

- 프라이버시를 보장하는 데이터 마이닝 : 개인이 자신의 데이터에 대한 권리를 가질 수 있게 하기 위해 데이터 마이닝에 대한 데이터 보호 기술과 적절한 정책에 대하여 연구한다.
- 데이터베이스 정책 도구 : 데이터베이스의 보안에 관하여 사용자 및 관리자가 개인정보 보호를 위해 데이터베이스의 접근 설정을 할 수 있도록 하고 누가 데이터베이스에 접근 권한을 가졌는지를 알 수 있도록

† 본 연구는 행정자치부에서 시행하고 정부혁신지방분권위원회 주관으로 한국전산원이 수행한 전자정부지원사업의 결과물입니다.

하기 위해 사용자 중심적으로 보완하려 한다.

- 신원절도와 신원보호 : 네트워크상에서 일어나는 많은 신원절도 유형에 대한 연구와 신원을 보호하기 위한 기술들에 대해 연구한다.

2.1.3 PORTIA 진행 현황

현재 PORTIA는 다양한 워크숍을 통해 민감한 데이터를 보호하기 위한 기술적인 사항들에 대해 논의하고 있으며 참여 대학교와 연구소에서는 개인정보보호에 관한 과목들이 개설되어 교육이 이루어지고 있다. 하지만, 아직까지 구체적인 기술개발은 이루어지지 않고 있으며, 관련된 이론적 연구만 이루어지고 있는 실정이다. 현재까지 개발된 소프트웨어로는 스푸드가드(spoofguard)와 패스워드해쉬(pwdhash) 등이 있다.

2.1.4 참여 대학교와 연구소의 프라이버시에 관한 과목

미국의 저명한 대학 중심으로 개인정보 및 개인정보보호와 관련한 많은 과목이 PORTIA 프로젝트의 지원금을 받아 이루어지고 있다.

표 2 프라이버시에 관한 교육 과목

대학교	과 목	내 용
스탠포드 대학교	데이터프라이버시에 대한 불안정한 기술들	데이터의 접근과 개인정보보호를 유지하기 위한 기술들에 대한 연구
	컴퓨터와 네트워크 보안	컴퓨터와 네트워크 보안에 대한 연구
	암호학 소개와 컴퓨터 보안	컴퓨터 보안에 사용되는 암호 기술의 이론과 응용
	컴퓨터 보안과 암호학에 관한 10가지 생각	컴퓨터 보안과 관련된 기초 암호학에 대한 신입생 세미나
예일 대학교	유선세계에서 민감한 정보	컴퓨터와 네트워크 사용의 증가에 따라 늘어나는 정보 제어에 대한 기술들
	정보시스템에서의 진보된 주제	새로운 정보 시스템 기술의 토대를 만들기 위한 다양한 개념을 제공
예일 법과 대학	PORTIA프로젝트의 법적인 전망	PORTIA 프로젝트의 법적인 관점에서의 논의
스티븐 기술 연구소	암호학의 기초	암호 시스템이 제공하는 서비스와 서비스를 얻기 위한 기술들
	암호 프로토콜	다양한 보안 프로토콜들과 다양한 공격 방법, 해결 방안
	보안 세미나	보안 관련 다양한 주제들을 가지고 열리는 세미나
뉴멕시코 대학	기술세계의 개인정보	프라이버시 침해사례와 보호

2.2 MIPA Project & Privacy/Data Protection Project

MIPA 프로젝트와 P/DP 프로젝트는 건강 관련 분야의 프라이버시를 보호하고, 건강보험 편이성 및 책임법(health insurance portability and accountability act, HIPAA)을 지원하기 위한 프로젝트이다. 이런 공통된 기반을 가진 두 프로젝트의 구성상의 특징들을 살펴봄으로써 의료계의 개인정보보호를 어떻게 이루어 나가고 있는지를 알 수 있다. 먼저 HIPPA의 개인정보 규정내용을 간략히 살펴본다.

2.2.1 건강보험 편이성 및 책임법

미국 보건사회복지부(health and human services, HSS)는 1996년 HIPAA에 부합하는 개인정보 표준을 제시하는 규정을 수립했다. 이것은 환자 정보(개인의 과거, 현재, 미래의 신체적, 정신적 건강에 대한 내용을 문서, 구두, 전자적인 형태로 전송 및 저장하는, 개인의 신원 확인이 가능한 정보)에 대한 전자통신의 사용에 관한 내용이다. 모든 전자통신은 공격당하기 쉬우므로 HHS는 환자의 개인정보를 보호할 표준을 수립했으며 이 법률의 몇 가지 준수사항은 다음과 같다.

- 보험업자 및 병원은 치료, 지불 또는 건강관리 조치에 대한 정보를 사용 또는 공개하는데 대한 서면동의를 얻어야 한다.
- 비밀 건강 정보의 사용과 공개는 개인의 동의, 권한위임 또는 특정한 공공정책의 목적에 대한 약정 없이 HIPAA가 지정한 기관으로부터 허가받을 수 있다.
- HIPAA가 지정한 단체는 필요한 정보를 최소량으로 하여 정보의 모든 사용과 공개가 제한되도록 보장해야 한다.
- HIPAA가 지정한 단체는 비즈니스 제휴자가 보안장치를 보유하고 있다면 제휴자에게 비밀 건강 정보를 공개할 수 있다.
- 환자들은 HIPAA가 지정한 단체의 개인정보 관행을 충분히 통지받아야 한다.
- 환자들은 HIPAA가 지정한 단체의 저장된 비밀 건강 정보에 접속할 권리를 갖고 있다.
- HIPAA가 지정한 단체는 행정상의 준수사항(프라이버시 직원 임명, 작업장 구성원 연수, 정보에 대한 행정적, 기술적, 물리적 안전장치 구축포함)을 실행해야 한다.

이와 같이, 이 법률은 환자의 프라이버시를 보장하고 건강 권익을 보호함으로써 거대 보험회사로부터 소비자들의 권익을 지킬 수 있다. 정부는 이 법률로써 우리의 프라이버시를 지키기 위해, 소비자 정보를 유출하려고

하는 일부 업계(주로 보험회사)를 간섭할 수 있다[2].

2.2.2 MIPA 프로젝트

미국의 존홉킨스 대학 Giuseppe Ateniese 교수를 중심으로 2002년 7월에 시작 된 MIPA(Medical Information Privacy Assurance) 프로젝트는 HIPAA가 위임한 일원화된 건강 정보 표준 개발을 촉진하기 위해 개인정보 기술과 프라이버시를 보호하는 인프라 구조 개발을 최종 목표로 한다. 다시 말하면, MIPA는 사용자가 익명으로 의료 관련 조직과 상호작용하는 시스템을 설계하고 실용화하는 것을 주된 목적으로 한다.

MIPA의 결과물은 아직 이론적 결과가 주를 이루며 다음과 같다. 관련 소프트웨어는 곧 출시될 예정이다.

- A Provably Secure Nyberg-Rueppel Signature Variant with Applications
- Identity-based Chameleon Hash and Applications
- Efficient Group Signatures without Trapdoors
- Anonymous E-Prescriptions
- Medical Information Privacy Assurance: Cryptographic and System Aspects

2.2.3 Privacy / Data Protection Project

2002년에 시작된 P/DP 프로젝트는 마이애미 대학의 Ethics Programs 중 하나이다. 이것은 개업의나 건강 관련 조직들이 HIPAA의 새로운 데이터 보호 요구사항에 호응할 수 있도록 도와주며, 대부분의 활동이 웹 사이트를 통한 교육으로 이루어진다.

이 프로젝트의 주된 내용은 웹 사이트를 통한 교육으로서, 건강관리와 관련된 프라이버시/데이터 보호에 관한 이슈들에 많은 공헌을 하고 있다.

P/DP 프로젝트의 결과물은 프라이버시와 보안과 관련된 보고서이다. 프라이버시와 관련된 보고서는 Health and Human Services의 미국 지사 시민 권리 사무국(office of civil rights, OCR)이 보유한 HIPAA 토픽에 관한 시리즈와 전자적인 데이터 통신을 위한 워킹그룹, Strategic national implementation project가 보유한 HIPAA의 프라이버시와 보안에 관련된 보고서 모음집이 있다. 보안과 관련된 보고서는 NIST(national institute for standards and technology), CSRC(computer security resource center)가 보유한 정보 시스템 보안에 관한 보고서 모음집이 있다.

2.3 PISA(Privacy Incorperated Software Agent)

2001년 1월 시작된 PISA는 유럽 여러 국가와 캐나다가 참여한 320만 달러 규모의 개인정보 관련 에이전트 구축 프로젝트이다. 이러한 PISA의 목표는 3년 내에 사용자를 대신하여 적합한 정보를 신속히 수집하는 ISA(intelligent software agent, 지능형 소프트웨어 에이전트)를 만드는 것이다.

2.3.1 PISA 구성원

PISA는 여러 국가의 정부 기관과 기업체 및 학술 단체가 참여한 프로젝트이다. PISA 프로젝트는 네덜란드, 벨기에, 이탈리아, 프랑스 등 EU를 중심으로 진행 중이고 특이한 사항은 비유럽국가인 캐나다도 참여하여 활발한 연구를 하고 있다는 것이다. PISA 프로젝트 참여 기관은 아래 표 3과 같다

표 3 PISA 참여기관

기관명	국가
Dutch Data Protection Authority	네덜란드
TNO(http://www.tno.nl)	네덜란드
Delft University of Technology (http://www.tudelft.nl/index.cfm)	네덜란드
GlobaSign(http://www.globalsign.com/)	벨기에
Finsa Consulting(http://www.finsa.it)	이탈리아
Sentient Machine Research (http://www.smr.nl/)	네덜란드
National Research Council Canada (http://www.nrc-cnrc.gc.ca)	캐나다
CIME(http://www.zks.net/en/)	프랑스

2.3.2 PISA 프로젝트에 요구되는 기술

PISA 프로젝트는 네트워크 환경에서 개인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 소프트웨어 에이전트 모델을 만들려는 것이 핵심이다. 따라서 PISA 프로젝트의 기본적인 모델은 인공지능 정보검색을 위한 에이전트 기술, 데이터 마이닝(data mining) 기법, 암호화 기법, 그리고 법적인 조건을 기술적인 단계로 만드는 시스템 설계 기술과 같은 여러 발전된 기술을 통합한 새로운 소프트웨어가 되어야 할 것이다.

2.3.3 PISA 진행 현황 및 결과

PISA 프로젝트는 ISA(intelligent software agent)를 만드는 것을 목표로 삼고 있고 매년 'Milestone'이라는 이름으로 연구결과를 발표하였다. 작년에 PISA 데몬 발표가 이미 끝이 났다. PISA 프로젝트가 시작된 2001년부터 발표되었던 해당 결과물의 양은 다양하고 방대하다. 중요한 점은 이러한 프로젝트를 통해 공통적인 ISAT 모델에 대해 모색해 보았지만, 구체적인 표준이 나오지 않은 상태이다. 프라이버시 관리자는 지능형 에이전트로 발전될 것임은 확실하다. 지

능형 에이전트는 차세대가 유비쿼터스 시대가 될 것이기에 더욱 더 중요한 기술이다. 우리나라 혹은 아시아권에서도 이에 대한 공동 연구 및 표준화 작업이 필요하다. PISA에서 논의된 연구 결과물에 대한 자세한 내용은 [3]을 참조한다.

2.4 P3P(platform for privacy preferences project)

인터넷 이용자의 개인정보보호에 대한 우려를 해결하기 위해 미국을 중심으로 형성된 조류중 하나는 기술적 대안, 즉, 프라이버시보호기술(PETs, privacy enhancing technologies)을 개발하는 인터넷 기업이고, 다른 하나는 정부와 소비자 단체 등 온라인상에서 사용자의 프라이버시를 보호하려는 전문가 집단이다. 이 두 그룹간의 접점으로 탄생하게 된 것이 OPS(open profiling standard)라고 할 수 있다. 1997년경 W3C는 eXtensible markup language(XML)를 어떻게 OPS에 사용할 것인지 고려하게 되었고, 결국 OPS는 P3P(platform for privacy preferences project)에 포함되게 되었다. 이로써 P3P 표준은 W3C에 의해 개발되어 인터넷상에서 개인정보보호를 위한 기술적 해결방안의 하나로 등장하게 되었다.

P3P(platform for privacy preferences project)는 사용자가 자신이 방문하는 웹 사이트에 주어지는 정보를 통제하도록 간단하고 자동화된 방식을 제공하는 새로운 산업 표준이다. 이것은 많은 선택 문항과 함께 웹 사이트의 개인정보 정책을 포괄한다. P3P 가능 브라우저들은 개인정보 정책에 대한 답변을 읽고 사용자 선호사항에 대한 정책과 비교할 수 있다.

P3P 기술은 자주 사용하는 MS 인터넷 익스플로어에 잘 포함되어 있다. 하지만 사용자의 쿠키 설정의 번거로움과 개인정보보호 기준 설정의 어려움 등이 큰 단점이다.

3. 프라이버시 침해 기술

프라이버시 침해 기술은 크게 합법적인 기술과 불법적인 기술로 나누어진다. 여기서 합법적인 기술이란 법적 규제에 벗어나 있는 것을 의미하며, 사용자의 부주위로 인해 정보를 얻는 행위 및 합법적인 수단을 통하여 사용자의 동의를 거친 후 정보를 수집하는 행위를 의미한다. 이에 반해 불법적인 기술이란, 미리 만들어진 프로그램이나 알려진 공격 기술들을 이용하여 사용자의 개인정보를 불법적으로 수집하는 기술을 말한다.

3.1 합법적인 기술

합법적인 프라이버시 침해 기술은 기존의 네트워크 기술을 이용하는 것으로써, 악의적인 해킹 툴을 이용하지 않고 자원 공유 및 인터넷 검색 기술 등을 이용하여 누구나 손쉽게 프라이버시 관련 정보를 획득 할 수 있다. 이러한 기술은 기본적으로 다음과 같은 모순점을 가진다.

- 웹 검색 기술의 성능과 개인의 프라이버시 정보 보호와의 모순성 : 웹 검색 기술의 성능을 높이기 위해서는 개인 프라이버시의 침해를 피할 수 없다. 따라서 개인의 프라이버시 침해를 줄이기 위해서는 웹 검색 기능의 성능을 낮추어야 하는데, 이것은 전체 웹 검색 서비스의 성능 저하를 가져온다. 기술과 프라이버시 보호 사이에 모순 및 트레이드오프(tradeoff)는 자연적인 현상으로 생각된다.
- 방어할 수 있는 기술의 부재 : 아직까지 위의 모순을 해결할 수 있는 기술은 존재하지 않는다. 따라서 기술적인 해결책에 의존하는 것 보다, 법적인 규제로 프라이버시 관련 정보가 웹에 돌아다니지 않도록 막는 것이 더 바람직하다. 그리고 이에 대한 활발한 논의가 선행되어야 할 것으로 보인다.

3.2 불법적인 기술

불법적인 기술의 대부분은 해킹 및 컴퓨터 바이러스이며, IT 기술 패러다임의 변화로 인해 앞으로 다양한 해킹 및 컴퓨터 바이러스 등이 등장할 것으로 예상된다.

3.3 개인정보 침해 기술 전망

앞으로도 IT 기술 변화에 따른 다양한 개인 프라이버시 침해 기술이 나타나고 더욱 발전될 것으로 전망된다. 이와 더불어 내부 사용자에 의한 프라이버시 유출 행위도 더욱 활발해지리라 예상된다. 아래 표에 프라이버시 침해 기술들을 요약하였다.

표 4 프라이버시 침해 기술들

대분류	중분류	소분류	해당 기술
합법적 기술	네트워크 기술이용	웹 검색 기술 자원 공유 기술	Google, Yahoo 파일공유, 쿠키
	자동화 시스템	신원 확인 시스템 감시 시스템 사용자 계정 시스템	사용자 정보 등록 및 저장 기술
불법적 기술	해킹 및 바이러스	시스템 침입 프로그램 취약점분석프로그램 스파이웨어	해킹 및 바이러스, 패킷분석도구들, Webbug
	오프라인 이용한 행위	산업스파이 내부공격자	침입 절도, 폭력 빼돌림

4. 프라이버시 보호 기술

본 절에서는 사용자들의 개인적인 정보들이 빠져나가는 것을 막는 PET(Privacy Enhancing Technology) 기술을 살펴본다. PET 기술은 크게 웹 기반, 네트워크 기반, 에이전트(agent) 기반 기술로 나누어진다.

4.1 웹 기반 기술

웹은 사용자들이 손쉽게 인터넷을 이용할 수 있게 해준 반면, 사용자들의 개인적인 정보가 사용자도 모르는 사이 빼앗기는 것 역시 가능하게 했다. 따라서 이러한 웹 환경에서, 웹 사용자에 관한 모든 정보가 숨겨져서 누구에게도 사용자에 관한 정보가 노출되지 않는 익명성을 제공하는 기술이 필요하게 되었으며, 이것은 웹을 기반으로 한 대부분의 PET 기술이 추구하는 공통의 목표이기도 하다.

웹 기반의 PET 기술은 크게 클라이언트(client)의 익명성을 제공하는 기술과 서버(server)의 익명성을 제공하는 기술로 나누어진다. 이러한 기술들은 Mix-net을 기본으로 하여 현실적으로 구현된 기술들이 많다.

4.1.1 Mix-net

Mix-net은 익명성을 제공하는 통신 채널의 전형적인 실행 방법으로 Chuam이 제안하였다[4]. Mix-net은 송신자가 메시지를 전송하기 위해서 구성된 모든 Mix들의 공개키 들이 필요하고, 송신자의 계산량 또한 크게 되는 단점이 존재한다.

그림 1은 Mix-net을 나타내며, 이에 대한 대략적인 설명은 다음과 같다.

우선 k개의 Mix 서버가 존재한다고 가정한다. n명의 송신자들을 $A_1,..,A_n$ 이라고 할 때, 송신자 A_i이 자신과 자신의 메시지 m_i와의 관계를 숨기고 메시지를 전송하고자 한다. 수신자 B_i의 공개키를 E_{B_i}라 하고, Mix 서버 S_i의 공개키 및 개인키를 (P_i, i)라고 한다. 여기서 서버 S_i의 역할은 각 송신자의 암호문을 복호화하여, 난수 성분을 제거한 후 그 결과들의 순서를 랜덤하게 출력하는 것이다.

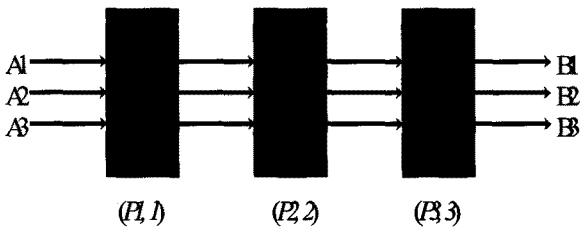


그림 1 Chuam이 제안한 Mix-net

설명의 편의를 위해, Mix 서버가 3개 있고 사용자 A1이 B1에게 메시지 Mi를 전달한다고 가정하자.

- [1단계] 각 송신자 A_i는 k개의 난수 R_1, R_2, R_3를 발생하여, 다음과 같은 암호문을 계산한 후 처음의 Mix 서버에게 전달한다.

$$E_{P1}(R_1, Adr_2, E_2'(R_2, Adr_3, E_3(R_3, Adr_{B1}, E_{Bi}(M_i))))$$

- [2단계] 최초의 Mix 서버 S_1는 수신한 암호문들을 복호화하고, 그 내용 중에서 난수 R_1을 제거한다. 난수 R_1의 의미는 확률적 공개키 사용을 의미한다. 복호화 한 내용 중 다음에 보내야 할 Mix 서버의 주소를 얻게 되고 그 주소로 나머지 암호화된 부분을 전달한다.

$$E_2(R_2, Adr_3, E_3(R_3, Adr_{B1}, E_{Bi}(M_i)))$$

- [3단계] 나머지 Mix 서버들은 차례로 단계 2와 같은 동작을 반복 수행한다.
- [4단계] 마지막으로, S_3는 $\{E_{Bi}(M_i)\}$를 사용자 Bi에게 전달하고 Bi는 자신의 개인키로 복호화 하여 메시지를 얻게 된다.

현실적으로 Mix-net을 기반으로 한 클라이언트와 서버의 익명성을 제공하는 기술은 Anonymizer, Onion Routing, Crowds, Janus, Rewebber, TAZ 등이 있다.

4.1.2 Mix-net의 연구 동향

하나는 Mix 서버의 메시지 포워딩 전략에 관련된 내용이고 또 하나는 Mix-net의 기능적 사항의 추가에 관한 내용이다. 2000년대 까지는 Mix 서버의 메시지 포워딩 전략을 나름대로 제시하고 이에 대한 메시지 연관성 및 익명성을 계산하는 연구들이 많이 이루어졌다. 최근에는 Mix-net의 다양한 기능 추가들에 대한 연구가 이루어지고 있다.

4.1.3 Mix-net의 향후 연구 과제

지금까지의 Mix-net 연구는 Mix 서버들이 각기 다른 batch strategy를 사용했을 때 발생하는 가능한 공격들과 이에 대한 익명성을 측정하는 논문들이 주를 이루었다. 이와 더불어, 다양한 Mix-net 기능들을 추가하고 이에 대한 익명성 및 비연결성을 증명하는 방향으로 연구가 이루어졌다. 하지만 지금까지 개발된 Mix-net 기술들을 차세대 USN(ubiquitous sensor network) 환경에서 그대로 쓰기에는 많은 무리가 있다. 예를 들어 공개키를 사용하는 Mix-net 구조는 엄청난 비용을 초래한다. 또한 USN의 센서 특성에 맞는 Mix-net 설계도 쉬운 일이 아니다. 유비쿼터스 센서 노드에서 라우팅 할 때 어떻게 입출력의 관계를 최소의 비용으로 숨기느냐 하는 문제는 아주 좋은 연구주제가 될 수 있을 것이다.

4.2 네트워크 기반 기술

프라이버시 침해 사고는 네트워크 환경에서 가장 빈번하게 발생한다. 이에 네트워크 환경의 특수성을 고려한 프라이버시를 보호하고 데이터를 안전하고 신뢰성 있게 전달하는 것을 목표로 하는 네트워크 기반 PET 기술은 중요하다. 잘 알려진 네트워크 기반 기술로 Proxy, 방화벽(firewall), 그리고 IDS 등이 존재한다.

4.2.1 방화벽 (firewall)

방화벽은 두 네트워크 사이의 트래픽을 제어하기 위해 구성된 시스템 또는 시스템들의 네트워크이다. 방화벽은 패킷 필터, 전용 프락시 서버, 스위치, 허브, 라우터 및 전용 서버 기반으로 다양하게 구현 가능하다.

방화벽의 기능을 지원하기 위해 요구되는 정보보호 서비스는 사용자 인증, 접근 제어, 트래픽 암호화, 감사 및 추적 기능, 인증된 사용자 추적 기능 등이 있다. 이러한 서비스들은 널리 알려져 있고 누구나 쉽게 이해할 수 있기 때문에, 구체적인 내용 설명은 생략한다.

4.2.2 침입탐지 시스템 (IDS: Intrusion Detection System)

IDS는 컴퓨터 시스템상의 비정상적인 사용, 오용, 남용 등의 불법 접근을 탐지, 분석하여 대응책을 알려주는 시스템이다. 그러나 IDS는 탐지된 침입에 대한 적극적 대응력 부족하고, 침입 자체 예방이 어려우며, 오탐 비율이 높고, 새로운 공격이나 알려지지 않은 공격은 탐지하지 못하는 것과 같은 단점이 존재한다. 이에 효율적이고 효과적인 대응을 위해 IDS를 다른 기술들과 함께 결합하는 형태인 ESM(Enterprise Security Management) 및 IPS(Intrusion Prevention System) 등을 사용하는 것을 권장하며, 이러한 기술을 개발하는 추세이다.

4.3 에이전트(agent) 기반 기술

에이전트는 특정 목적에 대하여 사용자를 대신하여 작업을 수행하는 자율적 프로세스로 독자적으로 존재하지 않고 운영체제나 네트워크와 같은 환경의 일부이거나 그 안에서 동작하는 소프트웨어로, 사용자나 다른 에이전트의 직접적인 지시나 간섭 없이도 스스로 판단하고 행동하는 자율성을 가지는 특성을 가지고 있다. 또한 사용자의 의도를 파악하여 계획을 세우고 학습을 통하여 새로운 지식을 터득하는 지능도 가지고 있다.

프라이버시 보호를 위한 에이전트는 사용자가 쉽게 파악 할 수 없는 인터넷상에서의 정보 유출에 대해 사용자를 대신하여 통제 해주는 역할을 하며, 그 기술로는 쿠키매니저(cookie manager), 에드브로커(ad blocker), 스파이웨어 필터(spyware filter) 등이 있다.

4.4 프라이버시 보호 기술 요약 및 발전방향

4.4.1 프라이버시 보호 기술 요약

PET 관련 Agent 기술은 보다 지능적이고 자동화된 기술로 발전해야 된다. 다음 표 5는 PET 관련 기술들에 대해 요약한 것이다.

표 5 PET 기술 분석 및 요약

분류	서비스	특징	기술
Web 기반 기술	Client의 익명성 제공	웹 사용자의 인터넷 이용에 관련된 정보를 숨기고, 암호화를 통한 데이터 트래픽의 내용 보호	Anonymizer Onion Routing Crowds
	Server의 익명성 제공	URL 암호화를 통한 익명성 제공, 브라우저 및 데이터 스트림의 암호화를 통한 데이터의 무결성 및 보안 제공	Janus Rewebber TAZ
Network 기반 기술	네트워크에서 정보의 안전성과 신뢰성 제공	접근 제어, 침입 탐지, 침입차단 패킷 및 침입 경로 추적 암호화와 복호화, 인증을 통한 안정성 제공	Proxy Firewall IDS
Agent 기반 기술	인터넷상의 정보유출에 대해 사용자를 대신 통제	다른 소프트웨어와는 다르게 에이전트는 스스로 판단하여 행동하는 자율성을 가진다.	Cookie manager Ad Blocker Spyware Filter

4.4.2 PET 기술 발전 방향

기존의 PET 기술들은 네트워크 환경에서 발생했던 여러 프라이버시 침해 문제가 발생할 때마다 프라이버시를 보호하려는 방안으로 개발되었다. 그러나 이러한 기술들은 앞으로 나타날 또 다른 프라이버시 침해 문제를 완벽하게 해결할 수 있다고 말할 수 없다. 따라서 앞으로 이슈가 되고 상용화되려는 인터넷 기술들을 면밀히 검토하고, 그 기술들이 상용화되기 전에 프라이버시 침해를 사전에 방지할 수 있는 방향 프라이버시 보호 기술은 발전해야 하며, 이러한 것은 법을 제정할 때도 감안되어야 한다.

5. 국내 환경에 적합한 프라이버시 보호 기술 정책 제시

지금까지 프라이버시 보호를 위한 기술적인 정책을 제시하기 위해, 프라이버시 침해 기술과 프라이버시 보호 기술을 살펴보았다. 이제 전 분야에 고루 적용될 수 있는 프라이버시 보호 기술을 살펴보기 위해, 각 분야별에서 공통의 취약점들을 뽑아내고, 이를 분석하여야 하지만, 이 부분은 양이 너무 방대하여 본 논문에서는 그 내용을 생략한다. 본 연구에서는 오직 공통적인 취약점 및 대응 기술을 분석하고 이를 바탕으로 현실적으로 적용 가능한 기술 정책을 제시한다. 대략적인 기술 정책

도출의 흐름을 정리하면 그림 2와 같다.

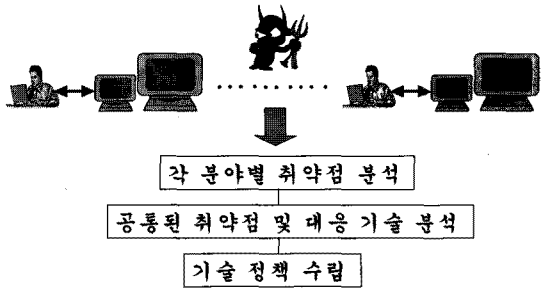


그림 2 기술정책 도출 방법

5.1 취약점

일반적인 공통된 취약점을 분석하기 위해, 모든 환경에 공통적으로 적용되는 일반적인 통신 모델을 설정해야 한다. 하지만, 국내의 금융, 의료, 공공기관, 통신 분야에 공통적으로 적용될 수 있는 일반적인 통신 모델을 찾는 것은 어려운 일이다. 이에 본 논문에서는 일반적인 통신 모델을 크게 사용자 측과 서버 측으로 나누고, 서버측은 또 다시 다른 서버들과 연결되어 있는 구조로 나누었다. 그리고 서버와 사용자 사이 구간도 중요하게 고려하였다. 그림 3은 이러한 일반적인 시스템 모델을 나타낸 것이다.

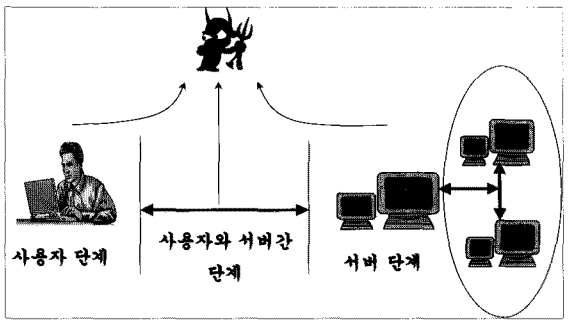


그림 3 일반적인 시스템 모델

5.1.1 사용자 단계의 취약점

사용자 단계의 취약점은 크게 외부자의 침입으로 인한 취약점과 내부자로 인해 발생되는 취약점으로 나눌 수 있다. 일반적으로 각 시스템 별로 요구하는 특징과 시스템들의 목적들이 상이하기 때문에, 모든 시스템에 적용 가능한 공통된 위협 사항을 찾는 것은 어렵다. 하지만, 외부자의 침입과 내부자에 의해 발생되는 취약점은 모든 시스템에 적용될 수 있는 공통된 취약점이라 할 수 있다. 외부자의 침입은 크게 컴퓨터 해킹의 시도 또는 컴퓨터 바이러스와 같은 악의적인 위협이 있다. 내부자로 인해 발생되는 취약점은 악의적인 목적을 가진 경우와 사용자의 부주의로 인한 경우에 가능하다.

5.1.2 서버 단계의 취약점

서버 단계에서의 취약점은 사용자 단계에서 발생했던 취약점 (컴퓨터 해킹 및 바이러스 및 내부자에 의한 위협)이 동일하게 적용된다. 이와 더불어 자연 재해 등 물리적, 환경적 원인으로 인해 사용자 정보가 유출될 수 있다.

5.1.3 사용자와 서버 단계에서의 취약점

사용자와 서버 단계에서의 취약점은 네트워크 통신에서 발생할 수 있는 취약점이다. 네트워크 통신에서는 불법적인 패킷이 중요한 위협요소이다. 왜냐하면, 불법적인 패킷이 곧 시스템 해킹과 연결되기 때문이다. 이를 위해 패킷에 대한 접근제어와 logging, 감사추적이 필요하다. 물론 전달되는 데이터의 기밀성도 중요하다. 이를 위해 데이터의 암호화 등이 이루어져야 할 것이다.

일반적으로 중요한 자료는 모두 암호화 되어 전달되어지기 때문에 서버와 사용자단계에서 전달되어지는 패킷을 보고 비밀정보를 획득하는 일은 결코 쉬운 일이 아니다. 하지만, 네트워크상의 모든 자료들을 암호화 하는 것은 이에 대한 암호화·복호화 모듈을 필요로 하고 이러한 공통된 프로그램이 전 시스템에 설치되어야 하므로 많은 비용을 요한다. 그러므로 암호화를 반드시 해야 할 적절한 곳과 상황을 정책적으로 명시할 필요가 있다. 또한, 네트워크상에서 불법적인 패킷 혹은 침입행위를 방지하기 위해 침입탐지 시스템 혹은 방화벽 설치를 권고할 수 있다.

5.1.4 관리적 취약점

인적 보안과 조직 구성의 부실로 인해 발생 가능한 취약점을 말한다. 인적 보안은 굉장히 중요한 이슈이다. 한 기관에서 계약기간이 완료되어 퇴사했을 경우, 그 사람은 자신이 업무를 통해 알았던 다른 고객의 민감 정보들을 유출해서는 안 된다. 실제로 이러한 것들로 인해서 고객의 정보 및 회사의 유용한 정보들이 많이 노출되고 있다. 이는 개인정보보호 서약서 등을 통해 계약 종료 후에도 개인정보보호가 노출되지 않도록 해야 할 것이다. 또한 서버구축과 웹 프로그래밍의 외주로 인해 내부 직원과 상관없이 외부 위탁자들에 의한 정보 유출도 간과해서는 안 된다. 위탁에 따른 통제가 필요하며, 적절한 규정 및 점검이 필요하다.

관리적 취약점은 보안 관리를 위한 인적구성이 적절히 이루어지지 않아서 발생하는 경우가 대부분이므로 개인정보보호 조직의 총괄 관리를 맡는 개인정보보호 책임자를 지정하여 하며, 꾸준한 보안 교육을 실시하여야 한다. 또한 각 부분별 담당자를 두어 사용자로부터 제기되는 개인정보에 관한 불만, 의견을 처리하며, 각 조직별 개인정보보호 시무지침을 작성 시행 점검해야 할 것이

다. 이러한 실무지침은 책임자의 승인 하에 관리 감독되어야 한다. 또한 계약기간이 완료되어 직원이 퇴사 했을 경우나 혹은 위탁업무와 관련한 직원에 대해서, 개인정보보호서약서등을 이용하여 계약종료 후에도 일정기간 개인정보의 노출이 이루어지지 않도록 할 수 있다.

5.2 기술정책 제시

기술정책은 법적으로 효력을 가질 수 있는 기술적 의무사항 및 권고사항들을 포함한다. 본 논문을 통해 일반적인 시스템에 공통적인 취약점들을 살펴보았고, 이에 대한 공통된 대응 기술 및 정책들을 나열하였다. 본 단락에서는 개인정보보호를 위해서 반드시 필요한 보편타당한 기술정책을 제시한다. 제시된 기술정책을 개인정보의 안전성을 위해 반드시 필요하지만, 현실적으로 구현하기에 무리가 있는 것도 있다. 크게 사용자 측과 서버 측으로 나누어서 기술정책을 제시한다. 사용자 측은 사용자 측에서 반드시 이행해야 할 기술정책이며, 서버측은 서버를 운용하는 기관에서 반드시 이행해야 할 기술정책이다.

5.2.1 사용자 측 기술정책 제시

사용자 측 기술정책은 컴퓨터 바이러스 방지 통제만을 설정하였다. 바이러스는 자신이 감염됨으로써 남에게 피해를 주게 된다. 또한 현재 IT 환경에서 정보보호 서비스 중 가장 중요한 것은 가용성이다. 바이러스를 통해 네트워크 서비스의 가용성을 상실하게 되면, 이로 인한 국가적 낭비는 엄청나다. 사용자 측에서 컴퓨터 바이러스와 관련된 기술정책은 타당하리라 본다. 자세한 기술정책은 다음 표 6과 같다.

표 6 사용자 측 기술 정책

기술 정책	의무 사항
컴퓨터 바이러스 방지 및 통제	○바이러스를 예방 및 통제 할 수 있는 백신 프로그램의 설치 및 주기적인 업데이트 의무화

5.2.2 서버 측 기술 정책 제시

서버측 기술 정책은 크게 불법적인 접근 방지, 자원에 대한 보안, 네트워크 보안, 내부 정보보호 계획 및 인적자원 보안 정책으로 나누어 살펴볼 수 있다.

- 불법적인 접근 방지 : 불법적인 접근은 크게 외부인의 서버 접속에 대한 접근 방지와 내부인의 권한 밖의 자원에 대한 접근 방지를 의미한다. 전자는 개인식별 및 인증 기술 정책을 둠으로써 방지할 수 있으며, 후자는 권한 관리 기술을 사용하여 해결 할 수 있다. 이와 더불어 접근 기록의 의무화도 반드시 이행되어야 할 부분이다. 표 7에서 보듯이, 제시된 기술정책은 대부분의 기관에서 적용하고 있는 보편적인 사항이다. 물론 현재 모든 기관이 이 사항들을 충실히 이행하고 있다고 볼 수는 없지만, 적어도 이러한 기술들은 실제 적용하기에 많은 시간과 비용이 소요되는 것이 아니므로, 현실적으로 정책을 집행하기에 보편타당한 기술 정책이 될 수 있을 것이다.
- 자원에 대한 보안 : 자원에 대한 보안은 크게 데이터베이스 보안과 문서 보안으로 나눌 수 있다. 이에 대한 기술 정책 및 의무사항은 표 8과 같다. 표 8에 언급된 DRM 부분은 기술정책으로 추진하기에 많은 시간이 비용이 필요할 지도 모른다. 하지만 기밀문서에 대해서는 많은 비용에도 불구하고 반드시 DRM 기술이 적용되어야 한다. DRM 기술을 적용하기 위한 현실적인 문제는 기밀문서에 대한 정확한 정의가 선행되어야 한다는 점이다. 자료 및 정보들을 사용자의 프라이버시와 관련해서 등급으로 나누는 작업은 많은 토론과 논의를 거쳐서 시급히 해결해야 할 사항이며, 그 결과 가장 중요하다고 판단된 기밀문서에 대해서는 많은 비용이 소모되더라도, 반드시 투자하여 보호해야함은 당연하다.

표 7 불법적인 접근 방지를 위한 기술 정책

기술 정책	의무 사항
식별·인증 기술 정책	○개인 식별 및 인증의 기술적 조치사항의 의무화 - 패스워드, 키 (PKI기술), 생체인식 정보를 이용한 인증기술 중 택일 하여 인증 기술 구현을 의무화 - 패스워드 입력 횟수 제한 : 패스워드 재입력 횟수에 대한 정책화 : 이로 인한 불법적인 접근 기록들 유지 의무화
계정 관리 기술 정책	○패스워드 관리 정책 의무화 - 휴면상태의 패스워드의 정기적인 점검 및 관리 - 패스워드 작성 규칙의 정책화 : 영어, 숫자, 특수기호를 혼용해서 작성할 것 ○아이디, 패스워드 전달 시 암호화 기술조치 의무화
권한 제어 및 관리 기술 정책	○사용자 별 자원 접근 기술의 의무화 - 사용자의 인증 정보 접근의 제한 : 사용자의 인증정보인 패스워드 접근 방지 의무화 - 직급별 자원 접근에 대한 권한 부여 : 권한 밖의 자원 접근 제한 ○개인 컴퓨터 암호 기능 설정의 의무화 - 컴퓨터 암호 기능 및 비밀번호 설정의 의무화 ○권한 제어에 대한 관리 - 정기적인 직급별 권한의 갱신 : 합리적인 권한 부여 정책에 대한 관리 감독 - 권한의 악용에 대한 정기적인 관리 감독의 의무화
접속 기록의 유지	○접속 기록의 정기적인 유지의 의무화 - 최소 3개월 이상 보관 ○접속 기록의 점검 감독의 의무화 - 접속 기록의 위·변조 방지 기술 의무화 - 접속기록의 정기적인 점검 및 분석

표 8 자원에 대한 보안

기술 정책	의무 사항
데이터 베이스 보안	○데이터베이스에 자료 저장 시 의무사항 - 자료의 암호화 - 정보보호책임자가 암/복호화 키 관리 ○데이터베이스에서 주요자료 출력 시 의무사항 - 자료 출력 시 사전 승인제도 실시 - 정보보호책임자의 승인 제도 실시 ○데이터베이스에서 주요자료 저장 시 의무사항 - 자료 저장 시 사전 승인제도 실시 - 정보보호책임자의 승인 제도 실시
문서 보안	○물리적 보안 - 건물 출입 시 문서의 이동을 통제함 ○기밀문서의 DRM 기술의 적용 - 허가된 사용자만 문서를 볼 수 있도록 함.
물리적/ 환경적 보안	○물리적 침입에 대비한 잠금장치 의무화 - 자료를 포함한 기기들의 물리적 보안 장치 의무화 ○건물 출입 시 사용자 인증 기술 의무화 - 생체인증 정보, 식별카드 등을 이용한 인증 기술 ○환경적 보안에 대한 대비책 의무화 - 자연재해로 인한 자료 손실 방지책 의무화 : 화재경보기, 소화기, 화재진압체계완비 : 무정전 전원 공급 장치 시설 완비

표 9 네트워크 보안

기술 정책	의무 사항
컴퓨터 해킹 및 바이러스 통제 기술 정책	○불법 패킷 탐지를 위한 기술적 조치의 의무화 - Firewall, IDS 설치의 의무화 ○조직 내 백신 프로그램 사용의 의무화 - 정기적인 업데이트의 의무화 ○정기적인 감독 관리의 의무화 - 바이러스 정보에 대한 주기적인 교육 - 백신 프로그램 올바른 사용의 정기적인 점검 ○침해 사고 대응 방법/절차 수립 - 비상연락망, 보고 대응절차와 관련된 침해사고 대응 체계의 마련 의무화 - 침해사고를 반드시 상급기관에 보고 의무화 ○컴퓨터 포렌식 기술의 의무화 - 침해 사고 발생 시 증거 확보의 의무화 - 증거 확보 기술의 의무화
자료의 기밀성 보장	○네트워크상에서 전달되는 기밀데이터의 암호화 기술 적용의 의무화 - PKI 기술을 이용한 암호화 기술 적용

- 네트워크 보안 : 컴퓨터 해킹 및 바이러스와 같은 네트워크상에서 발생할 수 있는 사고와 관련하여 제시할 수 있는 기술 정책으로는 불법 패킷 탐지 및 대응을 위한, IDS, 방화벽, 백신 프로그램의 설치 등이 있다. 또한 이러한 침해사고가 발생했을 때 대응체계를 마련해둠으로써, 피해를 최소화 할 수도 있을 것이다. 그리고 자료의 기밀성을 보장하기 위해서는 데이터의 암호화 기술 적용을 의무화하는 정책을 제시할 수 있다. 위의 표 9는 이에 대한 간략한 정리이다.
- 내부 정보보호 계획 및 인적 자원 보안 정책 : 내부 정보보호 계획은 프라이버시 보호와 관련한 실무지침을 의미한다. 이러한 실무지침을 각 조직별로 작성하고, 이의 실행을 관리 감독하면, 위반사항에 대한 법적인 처벌이 용이할 수 있다. 일반적으로 실무지침은 앞에서 언급한 기술정책을 반드시 반영하여야 한다. 자세한 내부 정보보호 계획 및 인적 자원 보안 정책에 대한 내용은 다음 표 10을 참고한다.

표 10 내부 정보보호 계획 및 인적 자원 보안 정책

기술정책	의무 사항
정보보호 전담조직 구성	○개인정보보호 책임자 및 담당자 지정 - 책임자 : 개인정보보호조직의 총괄 관리 : 개인정보보호 실무지침 승인 관리 - 담당자 : 실무지침의 작성, 시행 점검 : 개인정보에 관한 불만 고충 처리 ○개인정보보호 책임자 및 담당자의 정기적인 교육
정보보호 실무 지침 마련	○개인정보의 분류 및 정의 - 개인정보의 중요도, 영향도 분석 - 개인정보의 위험수준 분석 - 개인정보의 중요도에 따른 등급화 ○개인정보의 관리 방법 절차 마련 - 개인정보의 수집 이용의 항목 범위 설정 - 추가적인 개인정보보호 기술 정책 정립 - 특성화된 개인정보보호 기술 정책 수립 ○작성된 실무지침의 이행 및 감독 - 최고 경영층, 정보보호책임자의 승인 - 정보보호책임자의 실무 지침에 대한 감독
인적 보안	○담당자와 책임자, 임직원을 위한 보안 교육의 정기적인 실시의 의무화 ○개인정보보호 서약서의 의무화 - 입사 혹은 퇴사 시 개인정보보호 서약서를 통한 인적 보안의 의무화 - 위탁자들에 대해서도 개인정보보호 서약서를 통한 인적 보안 의무화 - 이에 대한 관리 감독의 의무화 : 개인정보보호 담당자의 책임

5. 결 론

프라이버시 침해 기술은 IT 기술의 진보와 더불어 고도로 다양화되고 지능화되고 있다. 이에 다수의 선진국은 프라이버시 침해로부터 국민의 권리를 보호하기 위한 프라이버시 보호 법률을 제정하였거나 제정 중에 있다. 본 연구는 프라이버시 보호 법 제정에 반드시 필요한 기술적 사항들을 뒷받침하는 것을 목표로 수행되었다.

본 연구에는 세계 각국에서 추진되었거나 추진 중인 프라이버시 보호 관련 프로젝트를 조사함으로써, 현재 동향을 파악하였다. 그리고 프라이버시 침해 기술과 프라이버시 보호 기술을 살펴봄으로써 정책 제시에 필요한 기본 지식을 제공하였다. 또한 공통된 취약점을 기반으로 한 현실에 적용 가능한 기술정책들을 제시하였다. 따라서 본 연구가 현재 IT 환경 그리고 차세대 IT 환경에서 프라이버시 보호와 관련된 법 제정에 반드시 필요한 기술적 검토 자료가 되리라 예상한다.

참고문헌

[1] The PORTIA Project, http://crypto.stanford.edu/portia

[2] G. Bahadur, W. Chan, and, C. Weber, "Privacy defended : protecting yourself online", 최진이 역, "프라이버시 보호하기 = 온라인 상에서 자신을 보호하기", 피어슨 에듀케이션 코리아, 2002.

[3] G.W. van Blarkom, J.J.Borking,and J.G. E.Olk, "Handbook of Privacy and Privacy-Enhancing Technologies : The case of intelligent Software Agents," PISA Consortium, 2003.

[4] D.Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms." In Communication of ACM, Vol. 24, No. 2, pp. 84-88, Feb. 1981.

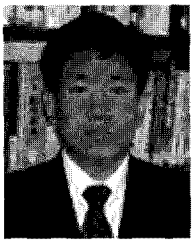
이 유 정

2003. 8 숙명여자대학교 수학통계학부 수학전공 졸업
2003. 9~현재 고려대학교 정보보호대학원 석사과정
관심분야 : 암호프로토콜, 센서네트워크 키 관리, Identity Management

변 진 욱

2001. 2 고려대학교 전산학과 졸업
2003. 2 고려대학교 정보보호대학원(석사)
2003. 3~현재 고려대학교 정보보호대학원 박사과정
관심분야 : 암호프로토콜, 키 교환, 익명성 연구, DB 보안

이 동 훈



1983. 8 고려대학교 경제학사
1987. 12 Oklahoma University 전산학(석사)
1992. 5 Oklahoma University 전산학(박사)
1992. 8 단국대학교 전자계산학과 전임강사
1993. 3~1997. 2 고려대학교 전산학과 조교수
1997. 3~2001. 2 고려대학교 전산학과 교수
2001. 2~현재 고려대학교 정보보호대학원 교수
관심분야 : 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술
E-mail : donghlee@korea.ac.kr