산업기술 보호를 위한 기술적 보안의 탐색적 연구

A Exploratory Study on R&D Strategies Industrial Technology Security

김경규*, 최서윤*, 허성혜*

Kyung-kyu Kim* , Seo Yun Choi* and Sunghye Hur*

요 약

첨단 산업기술의 보호를 통한 국제경쟁력 강화를 위해서는 국내 산업보안기술의 수준 및 기술경쟁력 등을 분석하고 나아가 개발과제의 발굴 및 지원방안을 수립함으로써, 산업보안기술 개발역량 강화 및 국제경쟁력 제고를 위한 정책수립이 필수적이다. 본 연구에서는 산업보안 기술의 전반적 동향 및 현황을 조사 및 분석하고, 급증하는 첨단 산업기술의 유출사고 예방 및 보안기술의 향상을 위해 기술적 보안 기술의 현재 수준분석과 국가적 차원의 산업보안 개발과제 도출을 진행하였다.

Abstract

To enhance international competitiveness through the protection of cutting-edge industrial technology, it is essential to establish the policy for strengthening ability to develop industrial security technology and raising international competitiveness. In this study we investigated and analysed not only the ecumenic trend but also the present condition, then we executed the deduction of the industrial security technology development program in a aspect of government and analysed the current status of the technical security technology for developing security technology and increasing leaks of the advanced industrial technology.

Key words : Industrial Security, Mail Security, Document Security, DB Security, Network Access Control, Contents Monitoring and Filtering

I. 산업기술 유출현황

2008년 국가정보원의 산업기밀보호센터에서 조사에 의하면, 국내 산업기술 유출 적발 건수는 2000년부터 2007년 12월까지 총 145건으로 이러한 산업기술이 모두 유출되었을 경우 약 95조원의 경제적 손실을 입었을 것으로 추산되고 있다. 연도별 산업기술 유출 적발현황을 살펴보면, 2003년 이전에는 산업기술 유출 적합이 10건 이하에 불과하던 것이, 2004년에는 26건, 2005년에는 29건, 2006년에는 31건, 2007년에는 32건으로 매년 증가하는 추세를 보이면서, 산업기술 보호를 위한 전략이 시급한 상황이다 [1],[2].

산업기술 유출의 주체는 크게 내부자와 외부인 등으로 나눌 수 있다. 내부자에 의한 산업기술 유출은

* 연세대학교 정보대학원(Graduate School of Information, Yonsei University)
· 교신저자(Corresponding Author): 허성혜
· 투고일자 : 2009년 1월 22일
· 심사(수정)일자 : 2009년 1월 23일 (수정일자 : 2009년 2월 9일)
· 게재일자 : 2009년 2월 28일

개인 컴퓨터 또는 업무시스템의 중요정보나 전자문서를 웹, 전자메일, 인터넷 메신저의 첨부형태로 유출하거나, 오프라인 문서의 경우 프린트, 복사물을 불법 유출하거나 팩스를 통하여 유출하는 것으로 조사되었다. 외부인에 의한 산업기술 유출의 경우 외부인이 네트워크를 통하여 시스템을 해킹하고 바이러스나 웜을 이용하여 전자정보를 유출하거나 사내에 무단 침입하여, 전자정보를 보관하고 있는 정보시스템 자산이나 프린트 및 복사기를 통해 생성된 오프라인 문서를 유출하는 것으로 조사되었다. 실제로 유지보수 등을 위해 사내에 출입한 외부인이 업무시스템의 데이터베이스에 접근하여 대규모 전자정보를 유출하거나 정보시스템 자산 및 오프라인 문서를 유출한 사례가 있었다 [1],[2].

그림 1. 산업기술 유출현황
Fig. 1. Trend of Industrial Data Leakage
(출처: 2008년 국가정보원 산업기밀센터 보고서)

이와 같은 산업기술 유출을 방지하기 위하여 국내 관련기관에서는 급증하는 첨단 산업기술의 불법유출을 방지하고 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지 하고자 산업보안기술의 개발지원 등을 포함한 '산업기술의 유출방지 및 보호에 관한 법률'을 2008년 4월에 시행하였다. 그러나 본 법률의 구체적인 적용을 위해서는 현재 국내외 산업기술 보호를 위한 현재의 기술적 보안의 수준분석과 이를 개선하기 위한 연구가 필수적이다. 따라서 본 연구에서는 국내 산업보안기술의 현주소와 기술경쟁력 등을 종합분석하고 개발과제의 발굴 및 지원방안을 수립함으로써 산업보안기술 개발역량 강화 및 국제경쟁력 제고를 위한 정책수립의 기초자료로 활용하고자 한다.

이를 위하여 산업기술 보호를 위한 요구사항을 분석하고 이를 해결하기 위한 방법으로 산업기술 보호를 위한 기술적 체계를 설계하였다. 설계된 기술적 체계에 따라 현재의 기술적 수준 및 한계성을 분석한 다음, 향후 개발 과제를 도출하였다.

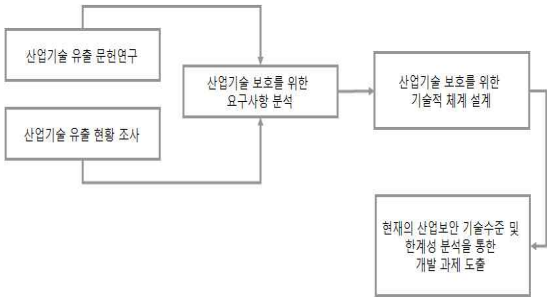

그림 2. 산업기술 보호를 위한 기술적 보안의 탐색적 연구방법론
Fig. 2. Research Methodology

Ⅱ. 산업보안 기술 요구사항 조사

본 연구에서는 실제적인 산업보안 기술의 요구사항을 조사하기 위하여, 2008년 8월 22일부터 10월 9일까지 국내 주요 산업보안기술 공급기업(15개)과 산업보안기술 수요기업(15개)을 방문하여 심층 인터뷰를 진행하였다. 조사된 주요한 산업보안 기술 요구사항은 다음과 같다.

o 조사결과 다양한 이동식 저장장치(Secure Digital Card, Compact Flash Card, Memory Stick 등) 및 통신방법(Infra-red Data Communications, Wireless Internet, Blue Tooth 등)이 출현할 때마다 이에 대응한 기술을 새롭게 개발하여야 함

o 일반 사무용 문서(워드 파일, 엑셀 파일, 파워포인트 파일)에 대한 보안기술은 안정화 수준까지 개발되었으나, 설계도면 및 프로그램 소스문서에 대한 보안기술은 아직 미진한 상태임

o 데이터베이스 보안기술은 성능문제로 인하여 암호화 방법보다는 접근통제 방법이 주로 활용되고 있으며, 불법적인 SQL 질의 문에 대하여 이를 정형화할 수 있는 기술이 요구됨

o 원격 컴퓨터에 대한 보안수준 측정모형은 아직 미진한 상태이며, 보안 수준을 통과한 컴퓨터에 대한 자원 활용 권한설정 및 통제방법에 대한 연구가 필요

함

o 현재 물리적 보안과 기술적 보안의 통합 운영되지 않기 때문에 연계지점에서 보안취약점이 발생되어짐

Ⅲ. 기술적 산업보안 기술 체계 설계

본 연구에서는 위험분석 과정 속에서 도출된 취약점 분석결과에 따라 취약점 문제를 해결하기 위한 기술을 설계하는 위험분석 기반 산업보안기술 설계 방법론을 적용하였다. 위험분석 기반 정보보호 기술개발 방법론은 정보자산 식별과 분석을 통하여 정보자산을 위협하는 요소들과 취약점들을 정리한 다음, 이러한 정보자산이 공격당했을 때의 영향과 위험에 대한 평가결과를 보안기술 개발 요구사항에 반영함으로써 기술적 산업보안기술 체계를 설계한다[4],[5],[6].

식별된 정보자산에 대한 취약점 분석을 바탕으로 문헌연구와 관련분야 전문가 집단(대학교수 3명, 보안기업 종사자 3명)을 통한 델파이 방법을 진행하여, 보안목적과 보안기술 등을 구분하여 표 1 과 같이 설계하였다. 참고적으로 델파이 방법은 전문가 집단으로부터 설문을 통하여 의견을 듣고 통계분석 결과를 다시 설문하여 의견을 수렴 집계하는 반복과정을 말한다. 이 방법은 각자의 전문가 의견을 수정할 기회가 주어지고, 다른 전문가의 의견을 활용할 수 있다는 점에서 매우 긍정적이며, 현재 기술 예측연구 분야에서는 90% 이상이 델파이방법을 사용할 정도로 보편적인 방법으로 자리 잡고 있다. 또한 전문가 집단의 참여를 통하여 신뢰성 있는 평가 결과를 얻을 수 있으며, 비교적 광범위하고 분석적인 견해를 제시하여 줄 수 있다.

산업기술에 대한 유출을 예방하는 목적의 메일 및 메신저 보안은 인터넷을 통한 전자메일 및 메신저의 내용을 암호화하고, 규칙에 의한 사전 필터링을 해주는 통제 기술이다. 이동 저장장치 보안은 개인용 컴퓨터에 연결될 수 있는 이동 저장장치(USB, Mobile Phone, Memory Card 등)에 대한 권한 통제를 수행하는 기술이다.

표 1. 기술적 산업보안기술 체계
Table 1. Industrial Security Framework

보안 목적		보안 기술	
예방 (Protection)	유출 통제 (Responsible Use)	메일 및 메신저 보안	
		기업 DRM	이동 저장장치 보안
	접근 통제 (Secure Use)		문서 보안
		DB 보안	DB 활동 모니터링 및 차단
			DB 암호화
		네트워크 접근제어	
모니터링 (AuditTrail)	콘텐츠 모니터링 및 필터링		

산업기술에 대한 접근을 통제하는 목적의 문서 보안은 기존의 파일 암호화를 기반으로 각종 권한관리 및 인증관리가 첨부되어 인증되지 않은 사람이나 권한이 없는 사람은 전자문서에 대한 접근을 불가능하게하며, 문서의 생성에서부터 저장장치 사이의 유통 및 폐기에 이르기까지의 전 과정에 보안 규칙을 적용하고 중요 문서의 유출경로까지 파악이 가능하게 함으로써 기밀문서 및 제품도면 등의 무단 유출을 방지하는 기술이다. DB 보안기술은 DB 활동 모니터링 및 차단기술과 DB 암호화 기술로 구성된다. DB 활동 모니터링 및 보호기술은 데이터베이스에 저장되어 있는 데이터를 대상으로 인가되지 않은 접근, 의도적인 정보의 변경이나 파괴 및 데이터의 일관성을 저해하는 우발적인 사고 등으로부터 데이터를 보호하는 기능을 한다. 또한 DB 암호화 기술은 데이터를 암호화하여 저장하고 필요시 암호화된 데이터를 복구하여 조회 변경하고, 다시 암호화하여 저장하는 방식이다. 네트워크 접근제어 기술은 사용자 단말이 네트워크에 접속하는 단계에서부터 단말의 보안 상태를 점검하여 보안정책에 부합하지 않는 단말에 대해 격리, 치료, 접속 허용 등 일련의 과정을 통해 가입자 단말과 내부 네트워크를 보호한다.

마지막으로 산업기술의 유통을 모니터링 하기위한 목적의 콘텐츠 모니터링 및 필터링 기술은 특정 응용 프로그램과 관련 비즈니스 규칙에 근거하여 모니터링하며, 네트워크상에서 민감한 정보의 부적절한 이동을 탐지한다.

Ⅳ. 현재의 산업기술 수준 및 한계성 분석

이동 저장장치 보안기술은 심층 인터뷰 조사결과 다양한 이동식 저장장치(Secure Digital Card, Compact Flash Card, Memory Stick 등) 및 통신방법(Infra-red Data Communications, Wireless Internet, Blue Tooth 등)이 출현할 때마다 이를 통제할 수 있는 기술이 개발되고 있으나 기존의 다른 장치들에 대한 통제 방법과 충돌문제가 발생하고 있다.

문서보안 기술은 도면 및 프로그램 소스 파일(파일크기가 매우 크며, 다양한 파일형식과 응용 프로그램 사이의 유기적인 상호연동이 필요, 프로세스를 구성하는 다단계 협업이 필요, 다양한 사내 및 사외 조직이 참여하는 것이 특징)의 경우 이에 접근통제가 제한적인 상태이며, 조직 내 파일을 안전하게 공유하기 위한 보안기술 개발이 미진한 상태다(현재는 파일 사용에 대한 이력 취합 불가, 조회 및 쓰기 등에 대한 이력 취합 불가, 파일을 사용자 컴퓨터로 다운로드 통제 불가, 다운로드 후 사용권한 통제 적용 불가).

DB 활동 모니터링 및 차단기술은 웹 어플리케이션 서버를 통하여 데이터베이스에 접근하는 경우, 데이터베이스 보안기술은 어느 클라이언트가 접속하였는지 알 수가 없기 때문에 따라서 사용자 단위에 접근통제가 아닌 웹 어플리케이션 단위의 접근통제만 이루어지고 있다. DB 암호화 기술은 데이터베이스를 암호화하는 경우, 인덱스 자체도 암호화되어 데이터 검색속도가 저하되며, 대용량 테이블을 암(복)호화할 경우 장시간이 소요되어 서비스 중단이 발생되고 있다.

네트워크 접근통제 기술은 조직의 규정에 따라 적정한 보안수준을 만족한 컴퓨터에서 사용자가 실행하는 악의적인 프로그램의 동작 및 행동을 차단하고, 조직의 보안정책 변경이나 컴퓨터의 건강상태 정보 변경에 따라 실시간으로 네트워크 접속을 통제할 수 있도록 통합적인(다른 보안시스템과의 연계한) 보안기술 개발을 요구하고 있다.

콘텐츠 모니터링 및 필터링 기술은 현재 일반 기업 및 공공기관의 경우 1 대의 웹 어플리케이션 서버의 작업내역에 대한 로그는 1시간에 1 GB 정도의 크기로 서버에 저장되고 있으나, 이러한 경우 약 1개월간 운영한 서버의 로그 자체 크기가 300 ~ 500 GB 정도의 대용량 데이터가 되며, 여기서 발생된 로그에서 사후 추적을 한다는 것은 매우 어려운 일이다.

Ⅴ. 산업보안 기술개발 전략 수립

앞서 설명한 바와 같이 산업기술을 보호하기 위하여 다양한 관점의 보안기술이 개발되고 있다. 그러나 유출통제를 목적으로 하는 기술들은 관리 작업이 많을 뿐만 아니라 정적인 관리가 이루어지고 있으며, 접근통제를 목적으로 하는 기술들은 정해진 형식의 파일에 대해서만 보호가 가능한 상태다. 또한 모니터링을 목적으로 하는 기술들은 탐지오류의 가능성이 있으며, 실시간 차단을 지원하지 못하고 있다 [5]. 따라서 향후 산업보안 기술은 조직의 업무프로세스에 기반 한 정책 중심의 기술을 개발할 필요가 있다. 따라서 본 연구에서는 관련분야 전문가 집단(대학교수 5명, 보안기업 전문가 5명)을 통한 델파이 방법을 적용하여 산업보안 기술개발 과제를 다음과 같이 도출하였다.

먼저 이 기종 이동장치 통제시스템은 제작사 및 작업환경과 무관하게 이동식 저장장치의 접근통제를 수행하면서, 외부로 정보를 전달할 경우 원격 컴퓨터에서도 정보에 대한 접근통제를 유지하는 기술이다. 세부적으로 이동식 저장장치 및 통신채널 통제기술 고도화(온라인 및 이동식 저장장치 간 복제 등을 통제, 이동식 저장장치에 부합된 전용 드라이버 사용에 무관한 접근통제)와 기밀성, 무결성, 강인성 모두를 지원하는 외부전송(전자메일 및 인터넷 메신저) 보안파일 생성 등으로 구성된다. 외부전송 보안파일은 첨부되는 문서의 암호화 및 외부 권한 자에게 복호화 키(비밀번호)를 별도로 전달함으로써, 보안파일을 받은 수신자는 자신의 단말기에 별도의 프로그램을 설치하지 않은 상태에서 단순한 파일의 실행만으로도 자신의 접근 허용범위 내에서 해당 문서를 열람하여 사용하게 한다.

산업기술 문서 통합보안 시스템은 전자문서에 대한 보안을 처리하는 기술들 사이에 호환성 및 보안성을 동시에 충족시키면서 업무 프로세스 상 독특한 특

성을 가지고 있는 설계도면 및 프로그램 소스파일의 보호를 지원한다. 참고적으로 설계도면 및 프로그램 소스 파일에 대한 보안기술은 관련분야 업무환경을 고려해 볼 때 다음과 같이 새로운 보안요구 사항들을 해결할 할 수 있어야 한다.

세부적으로 협업 가능한 산업기술 전자문서 보안기술은 산업기술 전자문서에 대한 사용자 및 응용 프로그램(예를 들어, 설계 프로그램)의 접근통제(인증 및 권한)를 동시에 진행할 수 있어야 하며, 기존의 사무용 문서보안 기술과 연동하여 통합적인 전자문서 보안기술이 개발되어야 한다. 호환 및 확장 가능한 문서보안 통합기술은 다른 기관 또는 동일기관 내 다른 조직에 문서를 송부할 경우, 수신자가 사용하고 있는 A사의 문서보안 시스템과 송신자가 사용하고 있는 B사의 문서보안 기술에 상호 운용 성을 현재 보장하지 못한 상태이기 때문에 문서보안 기술적용을 해제한 상태로 보내는 경우가 발생하는 것을 방지하기 위한 기술이다. 따라서 기관과 기관, 동일 기관 내 조직과 조직 사이에 문서유통의 전 과정 상에 정보유출을 통제할 수 있는 표준 API(Application Program Interface)의 개발이 필수적이다.

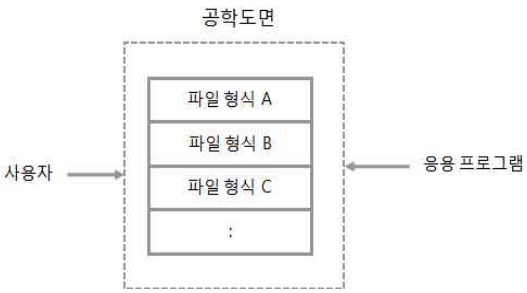

그림 3. 협업 가능한 산업기술 전자문서 보안기술
Fig. 3. Improved e Document Security

고성능 데이터베이스 보안 시스템은 웹 어플리케이션을 통한 우회적인 데이터베이스 접속방법이 가지고 있는 보안 취약점을 해결하고, 데이터베이스 필드를 암호화하면서 발생하는 사용자 업무처리 지연을 최소화(인덱스 검색 지원)하기 위한 보안기술을 말한다. 세부적으로 우회적 데이터베이스 접근탐지 및 차단기술은 웹 어플리케이션으로부터의 비정형화된 SQL 질의 문을 통제하고, 연결 지향형 네트워크 서비스를 제공하는 데이터베이스 보안서버가 장애가 발생되는 경우, 웹 어플리케이션 서버가 데이터베이스에 직접적으로 접속할 수 있는 가용성을 보장하는 기술이다.

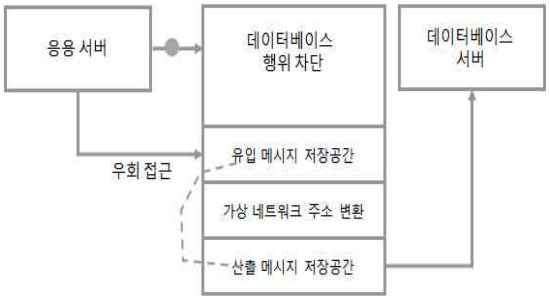

그림 4. 우회적 데이터베이스 접근탐지 및 차단기술
Fig. 4. Improved Database Security

빠른 속도의 데이터베이스 암(복)호화 및 검색기술은 데이터베이스 필드의 암(복)호화를 지원(Null 데이터 암호화도 포함)하는 안전한 키 관리(키를 파일 또는 테이블에 저장하지 않음)와 암호화된 인덱스를 사용하면서, 이와 동시에 인덱스를 통한 색인 검색을 지원(순차검색 발생을 최소화)한다.

마지막으로 역할기반 네트워크 앤드 포인트 보안 시스템은 원격으로 접속하는 컴퓨터들과의 비 호환성 문제(운영체제의 경우 MAC OS, Linux 등이 있으며, 단말기 형태의 경우 인터넷 전화기, 네트워크 프린터와 같은 non PC 등)를 해결하고, 네트워크 접근 통제 기술들 사이에 상호 운용을 보장할 수 있는 기술이다. 또한 조직 내 모든 사용자 그룹과 환경을 포괄하고 유연한 산업표준 기반보호를 구현하는 네트워크 접근 통제를 지원하게 된다.

VII. 산업보안 기술에 관한 탐색적 연구결과

첨단 산업기술의 보호를 통한 국제경쟁력 강화를 위해서는 국내 산업보안기술의 수준 및 기술경쟁력 등을 분석하고 나아가 개발과제의 발굴 및 지원방안을 수립함으로써, 산업보안기술 개발역량 강화 및 국제경쟁력 제고를 위한 정책수립이 필수적이다. 본 연구에서는 산업보안 기술의 전반적 동향 및 현황을 조사 및 분석하고, 급증하는 첨단 산업기술의 유출사고

예방 및 보안기술의 향상을 위해 기술적 보안 기술의 현재 수준분석과 국가적 차원의 산업보안 개발과제 도출을 진행하였다.

세부적으로 산업기술 유출현황을 분석하여 유출 주체, 경로 및 방법을 파악하고, 산업기술 자산식별과 함께 관련 문헌조사와 산업보안 기술 수요 및 공급업체를 방문함으로써 보안 요구사항 조사에 따른 산업기술 보호를 위한 기술적 체계를 설계하였다. 그 다음 전문가 집단을 통한 델파이 방법을 적용하여 세분화 된 기술개발과제를 도출하였다. 그 결과 이기종 이동저장장치 통제 시스템, 산업기술 문서 통합보안시스템, 고성능 데이터베이스 보안 시스템, 역할기반 네트워크 앤드 포인트 접근통제 시스템 등을 설계하였다.

본 연구의 결과는 향후 산업보안기술 개발역량 강화 및 국제경쟁력 제고를 위한 정책수립의 기초자료로 활용될 수 있을 것이며, 학계와 업계의 의견에 기초한 산업보안기술 체계는 산업기술 유출의 예방, 탐지, 대응에 대한 접근방법 및 수단을 제공할 수 있을 것으로 기대된다. 향후에는 본 연구결과를 바탕으로 산업기술 보호를 위한 물리적, 관리적 보안체계에 대한 연구와 함께 이를 통합하여 관리할 수 있는 산업기술 보호에 특화된 정보보안 관리체계(Information Security Management System for Industry Security) 개발이 요구된다.

참 고 문 헌

[1] 산업기밀보호센터, “첨단 산업기술 보호동향”, 9호, 국가정보원, 2008.

[2] 한국산업기술보호협회, “산업기술 보호를 위한 실태조사 보고서”, 2008.

[3] Dodson Rob, "Information Incident Management", Information Security Technical Report, 2001.

[4] Forte, Dario, "Information Security Assessment: Procedures and Methodology", *Computer Fraud & Security,* 2000.

[5] Gartner, "Hype Cycle for Governance, Risk and Compliance Technologies", 2008.

[6] Gartner, “Understanding Data Leakage”, 2007.

김 경 규 (金京圭)

1980년 : 서울대학교 경영학과(학사)
1984년 : University of Utah(M.B.A.)
1986년 : University of Utah(박사)
1986년~1990년 : Assistant Professor of Accounting and MIS, Penn State University
1989년~2001년 : 인하대학교 교수
1999년~2002년 : Associate Professor of Information Systems, University of Cincinnati
2001년 3월~현재 : 연세대학교 정보대학원 교수
관심분야 : 공급망관리, 유비쿼터스 비즈니스, 지식경영

최 서 윤 (崔瑞允)

2001년 8월 : 캘리포니아주립대학교 (San Jose) 응용미술(학사)
2004년 2월 : 연세대학교 정보대학원 멀티미디어(석사)
2004년 3월~2008년 12월 : 성신여자대학교, 호서대학교, 홍익대학교 출강
2007년 3월~현재 : 연세대학교 정보대학원 디지털문화컨텐츠 박사과정
관심분야 : 가상현실, 유비쿼터스 컴퓨팅, 저작권 보호

허 성 혜 (許成惠)

1999년 2월 : 이화여자대학교 국어국문학과(학사)
2004년 2월 : 연세대학교 정보대학원 정보시스템관리(석사)
2004년 8월~2005년 9월 : i2 technologies, Inc.
2007년 9월~현재 : 연세대학교 정보대학원 디지털 비즈니스 박사과정
관심분야 : 유비쿼터스 컴퓨팅, 정보경제학, 정보보호