情 報 保 護 學 會 誌
第19卷 第2號, 2009. 4

경북대학교 이동네트워크 정보보호기술 연구센터

문 상 재*

요 약

경북대학교 이동네트워크 정보보호기술 연구센터(Mobile Network Security Research Center, MSRC)는 2000년 8월 네트워크 분야의 IT 연구센터(지식경제부지정 ITRC)로 선정되어 2008년 12월까지 8년 4개월간의 연구센터로서의 연구, 개발, 인력양성 활동을 성공적으로 수행하였다. 경북대학교 문상재 교수를 중심으로 POSTECH, 부경대학교, 호서대학교, 동서대학교, 경남대학교 등 6개 대학 연간 11 여명의 교수진과 57 여명의 대학원생들은 물론, 국내외 정보보호 분야의 외부 전문가와 관련 산업체들의 활발한 협력 연구 활동으로 논문, 특허, 산학협력, 표준화 등의 부분에서 우수한 연구 실적들을 도출하며, 지식경제부의 IT 대학 육성 지원 사업을 성공적으로 마무리 하였다.

Ⅰ. 센터의 설립 목적

본 센터는 "유비쿼터스 네트워크 환경에서의 정보보호 서비스를 제공하기 위하여 유무선이 통합된 통신환경에서 단말기(멀티미디어 단말기, 컴퓨팅 단말기, RFID), 혹은 통신 서비스에 이동성을 부여하면서도 정보보호 서비스를 제공하는 차세대 핵심 기술을 개발"하는 것을 목표로 설립되었다. 이를 통해 정보보호 전문 인력을 양성하고 지적 재산권 확보, 국제 표준화 참여, 산학 연계, 그리고 국제 교류 등을 통한 국가 경쟁력을 강화하고자 한다.

Ⅱ. 센터의 구성

유비쿼터스 네트워크 환경에서의 정보보호 서비스를 제공하기 위해서는 다양한 분야의 전문 지식을 필요로 한다. 본 센터에서는 센터장(문상재 교수)을 중심으로 6개 대학의 교수 및 학생 연구진들 각자의 전문 분야와 능력에 맞추어 3개 세부 연구과제로 배정하여 전문 연구 활동을 하였다.

2.1 제 1 세부 과제

제 1세부과제는 "유비쿼터스 네트워크 무선 접속 보안기술 개발"이라는 세부 과제 목표 아래, 경북대학교(문상재 교수, 센터장, 세부과제책임), 동서대학교(이훈재 교수), 호서대학교(하재철 교수)의 삼각 연계에 의한 공동 연구를 수행하였다. 연구 분야는 암호프로세서의 물리적 공격 및 방어 기술과 유비쿼터스 네트워크 접속 보안 프로토콜로 나눌 수 있다.

- 암호프로세서의 물리적 공격 및 방어 기술 :
  스마트카드, RFID, USB 토큰 등과 같은 암호 장치의 물리적 해킹 공격에 대한 취약성을 분석하고, 이들의 방어 방법에 대해 연구한다.
- 유비쿼터스 네트워크 접속 보안 프로토콜 :
  유비쿼터스 환경에 적합하게 키 관리 프로토콜, ID 기반 프로토콜, 링크 암호 등의 보안 프로토콜을 개선하고 경량화에 연구력을 집중한다. 또한, 개발된 보안 프로토콜의 안전성을 검증하기 위한 정형화된 분석 방법에 대해 연구한다.

2.2 제 2 세부 과제

제 2세부과제는 "유비쿼터스 환경을 위한 네트워크 보안기반 기술 개발"이라는 세부 과제 목표 아래, POSTECH(이필중 교수-세부과제책임, 최영주 교수)과 부경대학교(이경현 교수)를 중심으로 공동 연구를 수행

* 경북대학교 이동네트워크 정보보호기술 연구센터 (sjmoon@knu.ac.kr)

하였다. 제 2세부 과제의 연구 분야는 크게 Ad-hoc 네트워크 및 센서 네트워크를 위한 암호 알고리듬 개발, 소규모 네트워크에서의 ID 기반 암호 시스템 개발, 유비쿼터스 환경을 위한 보안 기반 구조 개발 분야로 나눌 수 있다.

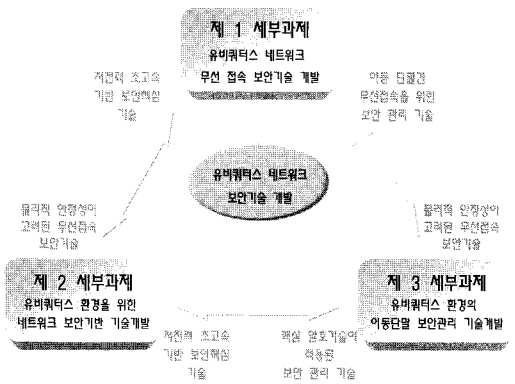
- Ad-hoc 네트워크 및 센서 네트워크를 위한 암호 알고리듬 개발 : Ad-hoc 네트워크와 센서 네트워크의 기본 모델과 Ad-hoc 네트워크와 센서네트워크에서의 보안 요구 사항을 분석하고 안전기준을 설정한다.
- 소규모 네트워크에서의 ID 기반 암호 시스템 개발: 초타원곡선을 이용한 암호 시스템 개선 방안을 연구하고 효율적인 pairing 알고리듬을 구현하여 ID-기반 암호 시스템에 응용한다.
- 유비쿼터스 환경을 위한 보안 기반 구조 개발 : 인증, 접근제어 기반 구조를 연구하고 이를 위한 핵심 암호 모듈을 개발한다. 또한 유비쿼터스 네트워크의 admission control 기술을 연구하고 credential 시스템을 개발한다.

2.3 제 3 세부 과제

제 3세부과제는 "유비쿼터스 환경의 이동 단말 보안 관리 기술 개발"이라는 세부 목표 아래, 경북대학교(김상욱 교수-세부과제책임, 유기영 교수, 고석주 교수, 문병인 교수)와 경남대학교(정민수 교수)가 주축이 되어 공동 연구를 수행하였다. 연구 분야는 크게 무선 연동용 보안 플랫폼 기술 개발, Multi-party key 및 유비쿼터스 환경에 적합한 고속암호 시스템 개발, 유비쿼터스형 보안 칩 내장형 초소형 미들웨어 기술개발, 이동 단말용 SCTP 프로토콜 전송 및 보안 기술 개발, 유비쿼터스 환경의 플랫폼을 위한 네트워크 프로세서의 보안 기술 연구 분야로 나눌 수 있다.

- 무선 연동용 보안 플랫폼 기술 개발 : 이동단말의 신뢰 관리 및 동적 협동 기술 분석하고 프로토타입을 설계한다. 유비쿼터스 환경의 이동 단말에 대한 보안관리 방법에 대해 연구하고 동적 협동 시스템 분석한 후 적합한 동적 협동 시스템을
- Multi-party key 및 유비쿼터스 환경에 적합한 고속암호 시스템 개발 : 유비쿼터스 환경을 위한 고속암호 시스템에 대해서 연구한다. 유비쿼터스 환경의 무선 네트워크를 위한 key 및 multi-key agreement 프로토콜을 연구하고, authentication 보안 프로토콜과 제어접근 기술들을 연구한다.
- 유비쿼터스형 보안 칩 내장형 초소형 미들웨어 기술개발 : 유비쿼터스 네트워크에 적합한 보안칩용 초소형 보안 매니저 기술을 개발한다. 이를 위해 보안칩용 초소형 VM 엔진을 개발하고 초소형 검증기 알고리듬에 대해 연구하여 초소형 검증기를 탑재한 로드매니저 기술을 개발한다.
- 이동 단말용 SCTP 프로토콜 전송 및 보안 기술 개발 : 이동 단말에 적용할 수 있는 SCTP 표준 프로토콜 분석하여 IPv6 기반의 IP 핸드오버 지원을 위한 mSCTP 이동성 기술을 개발한다. 또한 설계된 mSCTP 프로토콜을 실험을 통하여 핸드오버 성능을 검증한다.
- 유비쿼터스 환경의 플랫폼을 위한 네트워크 프로세서의 보안 기술 연구 : 유비쿼터스 환경에 사용이 가능하도록 보안 기능이 강화된 네트워크 프로세서 모델을 개발한다. 주로 ARM core-based 보안 기능을 가지는 네트워크 프로세서 구조를 개발한다.

본 연구센터에서 수행하는 각 세부과제들의 연관성을 나타낸 것이 [그림 1]이다.



〔그림 1〕 연구센터의 세부과제 구성

Ⅲ. 센터의 과제 추진 내용

3.1 센터의 연구 방향

경북대학교 ITRC 센터는 기반기술 중심 센터로서 이동네트워크 정보보호 기술에 기반이 되는 내용을 주로 연구하였다. 이를 위해 첫 번째, 국내외 학술 활동 및 표준화 활동 적극 참가하도록 권장하여 최신 기술을 습득이 용이하도록 하고, 연구 개발된 기술의 표준화 활동을 장려하였다. 두 번째, 국제 협력을 통해 연구 교류를 확대하였다. 호주, 중국, 대만, 싱가포르, 말레이시아, 오스트리아 등의 우수 정보보호 관련 연구 기관과의 공동 연구를 지속적으로 추진하여 상호 발전 관계를 유지하였다. 세 번째, 센터 내 자체 평가 시 기반 기술 중심으로 평가하여 인센티브를 차등 지급하였다. 기반기술 연구센터 역할을 수행하기 위해 센터 내의 자체 평가 기준도 조정을 하였으며, 각 평가 기준을 세부적으로 구체화하여 기반 기술 센터로서 선도적 역할을 할 수 있도록 하였다.

3.2 수요자 의견 반영을 위하여 추진한 전략

본 센터는 수요자의 의견을 적극 반영하여 활용하였다. 매년 코엑스에서 개최된 ITRC 포럼에 참가하여 그간의 개발된 연구 실적을 전시하였다. 전시회를 찾은 대학, 산업체, 연구소 종사자들과의 기술 면담을 통해 연구개발 기술을 소개하며 검증 받을 수 있었다. 실무경험이 부족한 연구 센터의 부족함을 파악할 수 있는 기회로 판단, 방문자들의 의견을 반영하는 기회로 활용하여 향 후 센터의 연구 방향을 기획하는데 적극 반영하였다.

또한 국내외 최신 기술 동향을 파악하기 위해서 비정기적으로 산업체, 연구 기관의 외부 전문가를 초청한 전문가 초청 세미나를 개최 하였다. 포괄적인 암호학에 대한 이해와 외부 전문가들의 지식을 접목하여 다양한 연구 과제들을 도출할 수 있었고, 실제 현장에서 사용되는 암호이론들과 이에 필요한 연구 분야들에 대한 지식도 습득할 수 있었다.

3.3 인력양성을 위하여 추진한 전략

우수한 정보보호 인력을 양성하기 위해서 산업체 인력 재교육 프로그램과 인적 자원의 해외 교류를 추진하고, 공동 연구를 통한 산업체 인력 양성 프로그램 추진하였다. 또한 본 센터에서는 학부생을 대상으로 실행하는 연구실 연수생 제도를 이용하여 정보보호 인력 저변 확대를 위해 노력 하였다.

3.4 센터의 기술축적을 위한 전략

센터에서 세계 수준의 기술을 축적하기 위한 여러 가지 시도들도 좋은 효과를 거두고 있다. 먼저, 센터에서 연구개발된 기술들의 DB화 및 문서화로 최신 연구 내용 공유하고, 센터 관련 연구 내용들과 경험을 후임 연구원에게 체계적으로 전수할 수 있게 하였다.

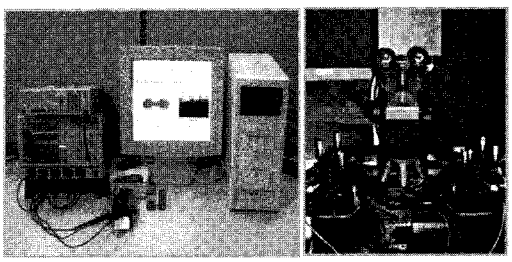
집중 연구 분야에 대한 장비 및 인력의 지속적인 지원하여 우수 실험 장비 확보는 물론이고 세계 수준의 기술을 유지할 수 있도록 하였다. 또한 해외 우수 연구기관들을 방문하여 기술 노하우를 습득, 최신 동향 파악 및 국제 협력을 위한 초석 마련하였다.

Ⅳ. 센터의 과제 추진 실적

4.1 정성적 실적

연구 센터의 우수 실적으로는 IC 카드와 같은 정보보호 장치에 대한 세계 수준의 물리적 해킹 공격 및 방어 기술을 보유하고 있다. 다수의 연구 실적과 함께 물리적 해킹을 위한 실험 환경을 센터 자체적으로 보유하고 있어서 암호용 칩, 스마트카드, RFID, USB token 등 다양한 정보보호 장치의 물리적 해킹 공격에 대한 안전성 테스트가 가능하다. [그림 2]는 센터에서 연구개발 중인 물리적 해킹 및 방어 대책에 관한 실험을 위한 장비들이다.

이와 더불어 USIM 모바일 보안 칩의 자바 COS를 개발하였는데 응용 프로그램을 적재 속도, 애플릿 선택 및 반응 속도 등이 획기적으로 개선되어 세계 수준의



〔그림 2〕 물리적 공격 및 방어 실험 장비

실적을 얻었다. 현재 최고 기술 보유사인 미국 Sun Microsystems 사의 제품과 비교하여 30%의 속도 개선 효과가 있으며, 관련 기술을 국내 산업체에 이전함은 물론이고 더 나아가 USIM을 이용한 웹 기반의 전자 화폐 시스템을 상품화하는데 성공하였다.

〔그림 3〕 고성능 자바 COS 및 USIM 프로그램 개발 툴

또한, 이와 같은 연구 결과를 국제 표준으로 연계시키는 노력을 경주하여 개발된 정보보호 관련 기술들이 국제 표준안에 채택되기도 하는 성과를 얻을 수 있었다. KCDSA(Korean Certificate-based Digital Signature Algorithm), EC-KCDSA (Korean Certificate-based Digital Signature Algorithm using Elliptic Curves) 등을 ISO/IEC 국제 표준에 포함시킨 것을 비롯하여, ISO/IEC, ITU-T에서 국제 표준화 확정 7건, 국제표준화 기고 52건의 활발한 표준화 활동을 수행하였다. 연구센터에 소속된 연구 교수님은 현재 ITU-T내의 표준 위원회에서 에디터로도 매우 활발한 활동을 하고 있다. 이외에도 유럽 ECRYPT 암호 공모전에 워드기반 스트림 암호인 "DRAGON"이 호주 QUT(Queensland University of Technology)와 공동으로 제출되어 최종 선정 직전 단계까지 경쟁하는 좋은 성과를 얻었다.

4.2 정량적 실적

센터장 경북대학교 문상재 교수를 중심으로 매년 11여명의 교수진과 57명의 대학원생들이 연구를 수행하였으며, 그 결과 IC 카드와 같은 정보 보호 장치에 대한 세계 수준의 물리적 해킹 공격 및 방어 기술과 USIM 모바일 보안 칩의 자바 COS를 개발하는 등 주요성과를 거두었다. 지난 8년 4개월간 "통신 서비스에 이동성을 부여하면서도 정보보호 서비스를 제공하는 차세대 핵심 기술을 개발하는 것"을 목표로 연구하여, [그림 4]에 나타낸 바와 같이 8년 4개월간 SCI급 논문 233 편, 국제 특허 5건을 포함한 특허 130건, 기술이전&지도 71 건, 배출인력 박사 26 명, 석사 113 명 등 괄목할 만한 연구 성과를 얻을 수 있었다.

〔그림 4〕 연구센터의 8년 4개월간 연구실적

V. 맺음말

경북대학교 이동네트워크 정보보호 연구 센터에서는 세계적 수준의 기술을 개발하기 위해서 특화된 부분에 연구력과 재정을 집중적으로 투자하였으며, 국내외 우수 연구 기관과 공동 협력을 통해 반 박자 빠르게 신기술을 개발하고자 노력하고 있다. 특히, 센터는 암호 칩에 대한 물리적 해킹 및 방어 기술과 USIM 모바일 보안 칩 관련 기술 분야에 재정과 인력을 집중 투자한 결과로, 세계 기술 수준과 어깨를 나란히 하고 있다. 또한, 우수 기술에 대한 기술 특허를 출원/등록하여 지적 재산권을 확보하고, 산업체에 관련 기술을 이전하여 상품화하는 등의 노력을 발 빠르게 진행하고 있다.

각 분야에서 독창적이면서 세계적 수준에 버금가는 기술을 활용한다면 신규 시스템 개발이나 응용력을 높이는데 기여할 것으로 여겨진다. 국내 기술로 개발된 제품은 유사 제품에 대한 외산 제품의 수입을 감소시켜 수입대체 효과를 볼 수 있으며 동시에 새로운 외국 시장으로의 진출을 도모하게 되므로 국내외 보안 시장 활성화에 크게 기여할 것으로 여겨진다. 센터는 정보의 이동성으로 이한 정보 가치의 상승 효과를 극대화하고 이를 신뢰성 있게 운영하기 위한 보안 기술을 확보하여 미래 유비쿼터스 시대에 대비하고 있다.

〔그림 5〕 경북대학교 이동네트워크 정보보호기술 연구센터 연구진