情 報 保 護 學 會 誌
第19卷 第4號, 2009. 8

정보보호 인증기술 연구 센터

정 한 재*, 원 동 호, 김 승 주

요 약

정보보호 인증기술 연구센터는 초경량 저비용의 인증 원천 기술 개발, 통합 인증 시스템 개발, 정보가전 네트워크에서의 인증기술 개발 등 정보보호를 위한 인증기술을 개발하기 위하여 연구 개발을 진행해왔다. 또한, 공통평가기준(CC, Common criteria) 및 CMVP(Cryptographic module verification program)와 같은 보안성 평가에 관한 많은 연구 및 과제 수행을 진행하였다. 특히 본 연구센터는 대학기관 중 국내 최초로 정보보호제품에 대한 CC인증 자문을 수행하였으며, 센터에 소속된 연구원들이 대학원생 최초로 수습 평가자 자격증을 취득하였다. 또한 2008년에는 지문인식 시스템 보호프로파일, 개방형 스마트카드 플랫폼 보호파일 등 총 6종의 보호프로파일을 개발하였다. 마지막으로 센터는 우수한 정보보호 인력 양성을 목표로 다양한 지원 및 제도를 운영하였다. 그 결과 다수의 우수 연구논문 발표, 국내외 특허 출원 및 등록, 기술이전 및 우수인력 배출 등 당초 목표 이상의 실적으로 달성하였다. 향후 정보보호 인증기술 연구센터는 지금까지 구축된 인증기술 및 보안기술과 산학협력 네트워크 등을 기반으로 우리나라가 인증기술 및 정보보호 산업의 강국으로 자리 잡는데 지속적으로 기여할 것으로 기대된다.

Ⅰ. 연 혁

본 연구센터는 총 8년간 연구를 수행하였으며, 2000년부터 2004년 까지 전자 상거래 환경에 활용될 수 있는 인증기술 개발 및 정보보안 분야의 전문 인력 배출을 목표로 하였다. 2단계는 2004년부터 2008년까지이며, 차세대 인증 및 데이터 접근제어 기술 개발을 통해 정보보안 분야의 전문 인력을 배출 하는 것이다. 본 센터를 통해 배출된 정보보호 전문가를 바탕으로 지속적인 연구 및 개발을 수행함으로써 정보보호 활성화를 지향하였다.

본 연구센터는 1차년도에 각 세부과제별로 기반 지식을 축적하고, 2, 3차년도에는 세부적인 기술 연구 및 개발을 수행하였으며, 4차년도에는 세부과제별 최종 목표를 달성하고 이를 통합하여 센터의 최종 목표를 달성하도록 연구를 진행하였다. 각 세부과제는 연구 센터의 추진 체계에 따라 센터의 목표와 부합하도록 다른 세부과제와 연계성 있는 연구를 수행하였다.

또한, 공통평가기준(CC, Common criteria) 및 CMVP (Cryptographic module verification program)와 같은 보안성 평가에 관한 많은 연구 및 과제 수행을 진행하였다. 특히 본 연구센터는 국내 대학기관 중 최초로 정보보호제품에 대한 CC인증 자문을 수행하였다. 이후에도 다수의 정보보호제품에 대한 CC 인증 자문을 수행하였으며, 2008년에는 지문인식 시스템 보호프로파일, 개방형 스마트카드 플랫폼 보호파일 등 총 6종의 보호프로파일을 개발하였다. 또한, 대학원생 중 최초로 센터에 속한 연구원들이 수습 평가자 자격증을 취득하였다.

본 연구센터는 연구 수행을 위한 고급 연구 인력을 갖추었으며, 적극적인 연구 활동을 통해 논문과 표준화 작업, 국내·외 특허 출원 및 등록에 심혈을 기울였다.

정보보호 인증기술 연구센터는 지금까지 구축된 인증기술 및 보안기술과 산학협력 네트워크 등을 기반으로 우리나라가 인증기술 및 정보보호 산업의 강국으로 자리 잡는데 지속적으로 기여할 것으로 기대된다.

* 성균관대학교 (hjjeong@security.re.kr)

Ⅱ. 연구 내용

2.1 인증 기술 개발

2.1.1 정보가전 네트워크에서의 인증 기술 개발

정보가전 네트워크란 PC, 이동전화, 디지털TV, 개인정보단말(PDA), 게임기 등 가정 내의 정보기기 간에 네트워크를 구축하여 디지털 데이터를 공유하고 광대역 통신을 사용하는 것을 뜻한다. 하지만 이러한 정보가전 네트워크는 복잡한 인증 방법으로 인한 편의성 저하, 초기 인증 단계에서의 보안 취약성 문제, 통일된 사용자 인증기술 부재, 다양한 기기와 프로토콜로 인한 상호 인증의 어려움 등의 문제점을 가지고 있다.

본 연구센터는 이러한 문제점을 해결하기 위해 정보가전 기기의 안전하고 빠른 등록 및 해제 기법, 보안성 있는 초기화 인증 기법, 하부네트워크에서 독립적인 사용자 인증기술, 정보가전기기 상호간의 인증 메커니즘 표준화 방향 등에 관하여 연구 개발 하였다.

2.1.2 초경량/저비용 인증 기술 개발

RFID/USN 환경에서는 RFID와 각종 센서 등을 이용해 각각의 개체를 식별하고 각종 정보를 수집한다. 이러한 기술들로 인해 사용자들은 좀 더 편리한 생활을, 각종 산업분야에서는 막대한 파급효과를 얻을 수 있을 것이라 예측 되지만 이러한 발전된 기술의 사용으로 인해 사용자의 프라이버시 침해문제, RFID tag의 위조 등을 통해 발생하는 경제적 손실 등이 나타날 수 있다.

본 연구센터는 이러한 문제를 해결하기위해 RFID 고속 인증기술 및 USN 환경에서의 센서 노드간 상호 인증 기술을 연구 개발 하였다. 더욱이 이를 통해 확보한 선도기술을 DRM 시스템에 적용하여 조직 외부로 자료와 문서가 불법 유출 되거나 무단 사용되는 것을 방지하는 문서유출 방지 시스템을 연구 개발하였다.

2.1.3 USN 환경에 적합한 AAA 기술 개발

유비쿼터스 센서 네트워크 환경이 실생활과 접목될 경우 새로운 산업 창출은 물론 국가의 경쟁력 강화에 커다란 도움이 될 수 있다. 그러나 유비쿼터스 센서 네트워크 환경은 기존의 환경과 통신방식, 인증 대상 요소의 변동, 네트워크 패러다임 자체가 달라 존재하는 인증 기술이나 AAA 기술들을 그대로 적용하는데 한계가 존재할 수 있으며, 이로 인해 개인의 사생활 침해와 같은 정보 인권 문제가 발생할 수 있다.

본 연구센터는 이러한 문제점을 해결하기 위해 인증 인자들의 인증보증레벨별 분류시스템을 연구 개발하였다. 또한 유비쿼터스 센서 네트워크 환경에 적합한 AAA 시스템 역시 연구 개발하였다.

2.1.4 통합 인증 시스템 개발

초고속 인터넷이 널리 보급되면서 전자상거래 등 많은 서비스들이 온라인을 통해서 이루어지게 되었다. 이러한 서비스를 보다 효율적으로 지원하기 위해서는 통합 인증 시스템 개발이 필수적이다.

본 연구센터에서는 호환성을 가지며 확장성을 지원할 수 있는 통합된 인증 시스템을 구축하기 위해 우선 인증서버 및 디렉토리 핵심 모듈, 인증서 경로 검증 시스템, 온라인 인증서 상태 검증 서버를 연구 개발하였다. 또한 스마트카드 기반의 인증 기법, 블루투스 기반의 인증 기법, 패스워드 기반의 인증 기법을 개발하고, 이렇게 개발된 기술들을 기반으로 통합 인증 시스템을 연구 개발 하였다.

2.2 보안성 평가 연구

2.2.1 CC 인증 자문

본 연구센터에서는 이론 및 IT제품의 보안성에 대한 실무를 겸할 수 있는 CC 및 CMVP와 관련된 연구 분야에 지속적인 노력을 통하여 국내 대학기관 중 최초로 정보보호제품에 대한 CC 인증 자문을 수행하였으며, 지금까지 다수의 정보보호제품에 대한 CC인증 자문을 진행해 왔다. 또한 CC 및 CMVP와 관련한 다양한 연구 과제를 수행하였다. 본 연구센터에서 수행된 CC 인증 자문과 CC 및 CMVP 관련 연구과제는 다음 [표 1]과 같다.

본 연구센터는 이러한 CC 인증 자문 및 관련 연구과제 경험을 바탕으로 국가정보원에서 주최하는 '정보보호제품 평가·인증 교육(일반/전문)' 교육과정에서 지난

2007년에 학생신분으로는 최초로 수습평가자 자격을 획득하기 시작하여 총 19명의 수습평가자를 배출해내었다.

〔표 1〕 CC 인증 자문 및 CC 및 CMVP 관련 연구과제

연구과제명	주관기간	수행기간
MULTOS 스마트카드 CC기반 평가 자문	삼성 SDS	2005
공통평가기준 3.0 분석	한국정보보호진흥원	2006
CC 인증 기술 자문	삼성전자	2006
OfficeServ 7400 CC 인증평가 자문	삼성전자	2006
Chakra v3.0 CC 기반 평가 제출물 작성	웨어밸리	2006
공통평가기준 3.1 기반 보호프로파일 개발	한국정보보호진흥원	2007
삼성전자 복합 프린터의 CC인증을 위한 평가 제출물 작성 및 자문	삼성전자	2007
비씨큐어 암호모듈 검증 제출물 작성	BCQRE	2009

2.2.2 보호프로파일 개발

본 연구센터는 CC인증 자문과 관련 연구과제 수행 등을 통하여 CC 및 CMVP 관련 지식과 경험을 습득하고 이를 바탕으로 2008년 무선랜 인증시스템 보호프로파일, 역할기반 접근통제시스템 보호프로파일, 네트워크 스팸메일차단 시스템 보호프로파일 등 총 6종의 보호프로파일을 개발하였다. 개발된 6종의 보호프로파일 및 등재일은 다음 [표 2]와 같다.

〔표 2〕 6종의 보호프로파일 개발[1]

보호프로파일	등재일
(CC v3.1) 무선랜 인증시스템 보호프로파일 V2.0	2008.09.19
(CC v3.1) 역할기반 접근통제시스템 보호프로파일 V2.0	2008.07.29
(CC v3.1) 네트워크 스팸메일차단시스템 보호프로파일 V2.0	2008.04.24
(CC v3.1) 지문인식시스템 보호프로파일 V2.0	2008.04.24
(CC v3.1) 개방형 스마트카드 플랫폼 보호프로파일 V2.0	2008.04.24
(CC v3.1) 침입차단시스템 보호프로파일 V2.0	2008.04.24

Ⅲ. 주요 연구 개발 성과

3.1 취약점 분석 보고

본 연구센터는 보다 안전한 정보화 사회를 만들기 위해 상용 정보보호 제품에 대한 취약점 분석을 수행하고, 이에 대한 결과를 발표하였다. 본 연구센터는 이를 통해 이러한 취약점에 의해서 발생할 수 있는 피해를 미연에 방지하고, 해당 제품들이 보다 안전하게 개발 될 수 있도록 하였다.

본 연구센터에서 보고한 취약점 분석은 다음과 같다.

〔표 3〕 상용시스템 취약성 분석

내용	날짜
국내 주요 메신저 취약점 분석[2]	2006.11
삭제된 공인인증서 복구 및 개인키 암호화 패스워드의 검출[3]	2007. 2
주민등록번호 대체수단에 대한 구현 취약점 분석[4]	2007. 4
보안 USB 플래시 드라이브 취약성 분석[5]	2007. 6
증권사 홈트레이딩 시스템(HTS)의 취약성 보고[6]	2007. 7

3.2 논문 실적

본 연구센터의 논문 실적은 다음과 같다.

〔표 4〕 논문 실적

사업단계	SCI급	국제 논문	국내 논문
1단계	84	77	268
2단계	140	107	206
합계	224	184	474

SCI급 논문 및 저명한 국제 학술대회에 논문을 투고하는 것을 목표로 하였으며, [표 4]와 같은 실적을 달성할 수 있었다.

3.3 특허 실적

본 연구센터의 특허실적은 다음과 같다.

1단계에 쌓여진 연구 경험을 바탕으로 2단계에 특허 출원 및 등록을 많이 달성할 수 있었다. 그리고 1단계

〔표 5〕 특허 실적

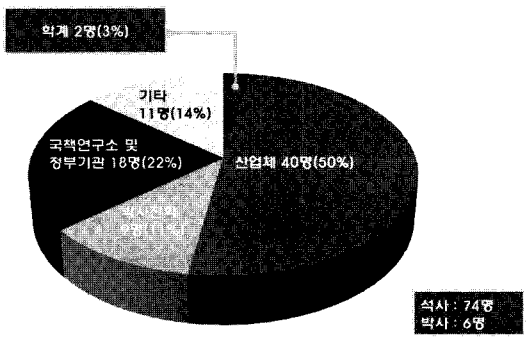
사업단계	출원	등록	합계
1단계	13	10	23
2단계	57(8)	15	72
합계	70	25	95

※ ( ) : 국제특허

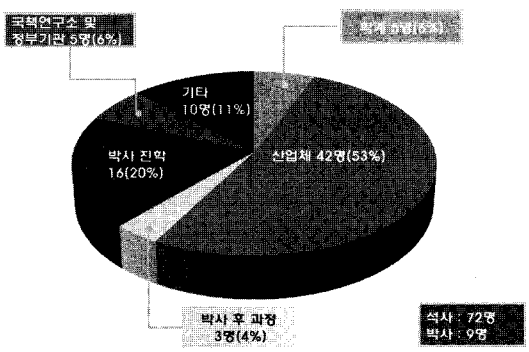
때 수행하지 못했던, 국제특허도 2단계에서 8건이나 출원했음을 알 수 있다.

3.4 인력양성 실적

본 연구센터의 1단계 수행기간에는 석사 74명, 박사 6명을 배출하였으며, 2단계에는 석사 72명, 박사 9명을 배출하였다. 8년 간 총 석사 146명, 박사 15명을 배출하여 인증기술 및 정보보안 기술 연구에 이바지 하였다. 배출된 연구 인력의 진로는 다음과 같았다.



〔그림 1〕 1단계 배출 인력의 진로



〔그림 2〕 2단계 배출 인력의 진로

3.5 기술 이전 및 상용화 실적

1단계 사업 기간에는 총 2건의 기술 이전 및 상용화가 이루어졌다.

〔표 6〕 1단계 기술 이전 및 상용화 실적

이전 기술 명	대상 기업	기술이전료
확장성 있는 보안 점검 시스템 개발	데이터게이트	8,000만원
개인 PC 접근제어 시스템의 구현 기술	이즈넷	2,000만원

2단계 사업 기간에도 1단계와 같이 총 2건의 기술 이전 및 상용화가 이루어졌다.

〔표 7〕 2단계 기술 이전 및 상용화 실적

이전 기술 명	대상 기업	기술이전료
신뢰성 향상을 위한 전자투표 영수증 발급 기술	(주)비씨큐어	900만원
도메인 DRM 라이선스의 암호화/복호화 시스템 및 그 암호화/복호화 방법	DRM Inside	2,000만원

3.6 기대효과

본 연구센터의 사회, 경제적 파급효과는 다음과 같이 나누어 볼 수 있다.

3.6.1 개발기술의 경제적 파급효과

1단계 사업기간의 연구를 통해 전자상거래에서 사용되는 인증기술을 진일보시킴으로써 유·무선 인터넷상의 전자상거래를 더욱 활성화시킬 수 있는 기반이 될 것이다. 또한, 인터넷 거래는 중간경로를 거치지 않고 직접적으로 거래가 이루어지므로 제품의 가격 인하는 물론, 시장경제의 활성화를 가져올 수 있을 것으로 기대된다. 또한 일반 상거래가 전자상거래로 옮겨짐으로써 산업구조의 변화가 일어나며, 기업의 새로운 비즈니스 기회 창출과 서비스의 개발을 통해서 기업 경쟁력이 강화될 것으로 기대할 수 있다.

2단계 사업기간에는 차세대 인증기술을 이용한 전자투표 시스템은 투표 기간 중 전국 어디에서든지 투표할

수 있어 투표율 상승을 도모할 수 있으며, 선거 관리 비용의 20~25%를 차지하는 일회성 투/개표 관리 비용을 절감할 수 있을 것으로 기대된다. 그리고 AAA 기술의 부재로 지연되었던 USN 환경에 적합한 어플리케이션 개발에 박차를 가할 수 있으며, 관련 산업의 발전으로 USN의 보급화를 촉진시켜 5년 이내에 실용적인 효과를 거둘 수 있을 것으로 기대할 수 있다. 또한, 정보가전 네트워크의 인증기술이 순조롭게 개발될 경우전국 70%이상의 가구에서 가정 내 통신망, 상호연동 미들웨어, 홈 네트워킹 기기를 이용할 것으로 기대되고 이에 따른 막대한 수입 창출이 예상할 수 있다. 마지막으로 사내 문서 유출 방지 시스템을 사용할 경우 침입탐지 또는 방지시스템 구축에 들어가는 비용을 절약함으로써 안정적인 USN 인프라 환경구축을 위한 핵심 기술을 확보할 수 있고, 핵심 기술을 이용하여 직접적인 이익뿐만 아니라 기술 수출로 인하여 기술료 등의 추가 수입을 얻을 수 있을 것으로 기대할 수 있다.

3.6.2 산업체로의 기술이전

본 연구 과제에서는 개발된 기술들은 단순 학술 연구에만 머물지 않고, 상용화 및 산업체로의 100% 기술 이전을 통해 국내 정보보호 분야의 인증기술 선진화에 기여할 수 있다. 그리고 이러한 계획이 활발하게 진행될 경우 각 업체들은 국내는 물론 세계적으로도 정보보호 분야의 인증기술에 관하여 앞서가는 최신의 기술을 보유한 기업으로 인정받을 수 있고, 향 후 5년 이상의 성장 가능한 토대를 마련할 수 있을 것으로 기대된다.

3.6.3 연구 인력의 재교육

본 연구센터에서는 매 학기 10명 이상의 분야별 정보보호 분야의 산업체 전문 인력 및 학계의 전문 인사를 초청하여 세미나 등을 통하여 정보보호 교육을 정기적으로 실시하였다. 이로써 실제 산업체에서 요구되는 기술과 연구되고 있는 기술의 견해차를 좁히고 기술의 상용화에 더 접근할 수 있을 것으로 기대된다. 또한 최근 기술의 동향 및 흐름, 비전 등의 정보를 신속하게 접하여 발전하는 기술과 맞물려 발전할 수 있는 기회를 제공하였다. 이를 통해 새로운 기술을 습득하여 산업현장에 빠르게 적용함으로써 선점 효과를 가질 뿐만 아니라 고부가 가치의 상품을 창출할 수 있을 것으로 기대된다.

Ⅳ. 결 론

본 연구센터의 차세대 인증 및 데이터 접근제어 기술 개발 및 정보보안 분야의 전문인력을 배출 하는 것을 목표로 2000년부터 2008년까지 총 8년여 동안 많은 노력을 기울여왔다. 그 결과 초경량 저비용 인증원천기술 등 다수의 기술을 개발 하였으며, 2004년부터 2008년까지 박사 11명, 석사 92명, 총 103명의 연구 인력을 배출하였다. 또한, 총 91건의 특허, 총 10건의 SCIE 급 논문의 실적을 달성하였다.

앞으로, 정보보호 인증기술 연구센터는 그 동안의 정부지원으로 구축된 인증기술 연구 개발 인프라 및 CC와 CMVP에 대한 연구 경험을 통한 보안성평가, 산업체와의 다양한 인프라를 활용하여 유비쿼터스 환경에 적합한 보안기술 개발에 집중할 계획이다. 그리고 인증기술 개발뿐만 아니라 우수한 지역인재의 발굴과 양성 임무를 지속적으로 수행할 계획이다.

참고문헌

[1] IT보안인증사무국, http://www.kecs.go.kr.

[2] 신동휘, 최윤성, 박상준, 김승주, 원동호, "네이트온 메신저의 사용자 인증 메커니즘에 대한 취약점 분석", *정보보호학회논문지* 17(1), pp. 67-80, 2007. 2.

[3] 최윤성, 이영교, 이윤호, 박상준, 양형규, 김승주, 원동호, "삭제된 공인인증서의 복구 및 개인키 암호화 패스워드의 검출", *정보보호학회논문지* 17(1), pp. 41-55, 2007. 2.

[4] 최윤성, 이윤호, 김승주, 원동호, "주민등록번호 대체수단에 대한 구현 취약점 분석", *정보보호학회논문지* 17(2), pp. 145-185, 2007. 4.

[5] 정한재, 최윤성, 전웅렬, 양비, 김승주, 원동호, "보안 USB 플래시 드라이브의 취약점 분석과 CC v3.1 기반의 보호프로파일 개발", *정보보호학회논문지* 17(6), pp. 99-119, 2007. 12.

[6] 이윤영, 최해랑, 한정훈, 홍수민, 이성진, 신동휘, 김승주, 원동호 "홈트레이딩 시스템 서비스의 보안 취약점 분석 및 평가기준 제안", *정보보호학회논문지*, 18(1), pp. 115-137, 2008. 2.

〈著者紹介〉

정 한 재 (Hanjae Jeong)

2006년: 성균관대학교 정보통신공학부 졸업(학사)
2008년: 성균관대학교 대학원 전자전기컴퓨터공학과 졸업(공학석사)
2008년~현재: 성균관대학교 대학원 휴대폰학과 박사과정 재학 중
<관심분야> 정보보호, 보안성평가, 무선네트워크

원 동 호 (Dongho Won)

정회원

1976년~1988년: 성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년: 한국전자통신연구원 전임연구원
1985년~1986년: 일본 동경공업대 객원연구원
1988년~2003년: 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년~1998년: 국무총리실 정보화추진위원회 자문위원
2002년~2003년: 한국정보보호학회장
2002년~현재: 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT감사 자문위원
2007년~현재: 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장
<관심분야> 암호이론, 정보이론, 정보보호

김 승 주 (Seungjoo Kim)

정회원

1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: 한국정보보호진흥원(KISA) 팀장
2004년~현재: 성균관대학교 정보통신공학부 교수
2001년~현재: 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현재: 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성평가, PET