情 報 保 護 學 會 誌
第19卷 第2號, 2009. 4

침입 감내, 대응 및 방지를 위한 시스템 보안기술 개발

노 봉 남*, 이 형 효**

요 약

시스템보안연구센터는 침입감내, 대응 및 방지에 필요한 시스템보안분야의 원천기술을 개발하고 정보보호업체와 함께 해당 기술을 상용화하는 것을 목표로 연구개발을 진행해 왔다. 산학일체형 연구교육모델을 정립하고 실천하여 우수한 정보보호인력을 양성함으로써 정보보호분야 IT고급인력양성이라는 교육적 목표와 함께 시스템보안분야 원천기술 확보 및 제품개발에 기여하는 산업적 효과를 얻고자 노력해 왔다. 참여교수와 대학원생, 정보보호 산업체 인력들의 8년간 연구개발노력으로 시스템분야 보안제품 상용화와 기술이전, 연구논문발표와 특허 등록, 우수인력 배출 등 여러 지표에서 당초 목표 이상의 실적을 달성하였으며, 향후 지금까지 구축된 시스템보안분야 기술개발능력과 산학협력 네트워크를 기반으로 우리나라가 지식정보보안산업 강국으로 자리잡는데 지속적으로 기여할 것으로 기대된다.

Ⅰ. 연 혁

시스템보안연구센터(센터장: 전남대학교 노봉남교수)는 2000년 8월 IT고급인력양성을 목표로 한 대학IT연구센터 지원사업의 시스템보안분야 연구센터로 선정되어 당해 9월 전남대학교 내에 '리눅스 시스템 보안연구센터'를 개소하면서 시스템보안분야의 원천기술 개발과 상용화를 위한 연구를 시작하였다.

2000년부터 2008년까지 진행된 총 8년의 1, 2단계 지원사업 기간 중 전남대학교를 주관대학으로 하여 광주과학기술원, 목포대학교, 전북대학교, 원광대학교 등 호남지역 대학 뿐만 아니라 남서울대학교, 성균관대학교, 숭실대학교, 연세대학교, 인천대학교, 포항공과대학교, 한국항공대학교, 한남대학교 등 시스템보안 분야를 연구하는 전국의 정보보호 전공 교수와 석·박사과정 대학원생이 연구개발사업에 참여하였다.

또한 산학협력 중심센터인 시스템보안연구센터의 연구개발주제 발굴과 시스템보안연구센터에서 개발된 연구결과의 상용화를 추진하기 위해 비트컴퓨터, 시큐브, 나우컴, 정보보호기술, 안랩시큐브레인, 인젠, 이글루시큐리티, 파이널데이터 등 국내 주요 정보보호업체와 산학협력세미나 개최, 기술지도 및 기술전수 등을 통해 긴밀한 산학협력체계를 유지, 발전시켜왔다.

그리고 한국정보보호진흥원, 한국전자통신연구원, 국가보안기술연구소 등 국내 정보보호 연구기관과의 공동연구를 통해 시스템분야 최신기술 표준화 및 발전동향에 관해 정보교류를 진행해 왔고, 미국 UNCC (University of North Carolina, Charlotte), Pittsburgh 대학, CMU CyLab, 러시아 St. Petersburg 대학 등과 인력파견 및 기술교류 세미나를 통해 시스템 보안기술 연구개발 관련 해외 최신동향을 파악하여 센터 연구개발 목표설정과 진행에 반영하였다.

본 고에서는 시스템보안연구센터가 지난 2000년부터 8년간 진행한 시스템보안분야 주요 연구내용과 센터 운영의 특징, 주요 연구성과를 정리한다. 마지막으로 시스템보안연구센터가 기여한 사회경제적, 기술적 효과에 대하여 기술한다.

Ⅱ. 연구 주제 및 운영 특성

2.1 연구주제

시스템보안연구센터는 '산학일체형 연구교육 모델'을 기반으로 '공개 S/W 원천기술 연구'를 통해 '침입감

* 전남대학교 전자컴퓨터공학부 (bbong@jnu.ac.kr)
** 원광대학교 정보·전자상거래학부, 정보과학연구소 (hlee@wonkwang.ac.kr)

내, 대응 및 방지 보안기술 상용화'를 목표로 연구개발을 진행해 왔다.

시스템보안연구센터가 지난 8년간 수행한 시스템보안 분야 연구주제는 크게 침입감내, 대응, 방지 분야로 분류될 수 있다([표 1] 참조).

〔표 1〕 센터 주요 연구개발 내용

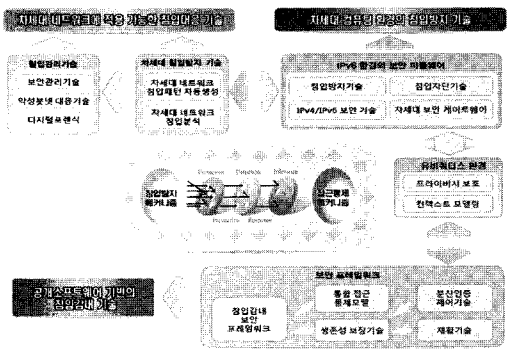
분야	주요 연구개발 주제
침입 감내	보안운영체제를 지원하는 침입감내기술 다양한 접근통제정책을 지원하는 보안미들웨어 개발 침입감내를 위한 통합 접근통제 프레임워크 개발 U-서비스 생존성 제고를 위한 서비스 브로커 개발 보안재활을 위한 경량화된 침입감내기술 개발
침입 대응	침입패턴 자동생성 및 정형화, 시뮬레이션 기술 개발 악성봇넷 대응 및 실용화된 디지털 포렌식 기술 개발 UTM기반 통합 보안관리시스템 개발 IPv4/IPv6 네트워크 환경의 악성행위 척도, 패턴 개발 휴대폰 증거수집을 위한 모바일 포렌식 기술 개발
침입 방지	차세대 컴퓨팅 환경을 위한 통합 보안 미들웨어 개발 프라이버시 보호를 위한 DB 보안게이트웨이 개발 IPv6 환경의 보안 미들웨어 개발 IPv6지원 네트워크기반 침입방지시스템 개발 혼재 네트워크에서 공격 및 대응기술 개발

침입감내 연구분야의 대표적 연구주제는 강제적접근통제(MAC: Mandatory Access Control) 정책과 역할기반 접근통제(RBAC: Role-Based Access Control) 정책을 모두 표현할 수 있는 개체-관계 기반의 새로운 통합 접근통제모델인 SEEN(SEcuity ENtitiy)의 개발과 구현이다. 이 연구에서는 SEEN 모델에 적합한 정책언어를 설계하고 보안정책 점검과 검증 시스템을 구현하여 보안관리자들이 보다 편리하게 일관성있는 보안정책을 작성할 수 있도록 하였다. SEEN 모델은 한중일 공개 보안운영체제 개발 프로젝트에 채택되어 표준화 주도뿐만 아니라 보안운영체제 분야의 기술우수성을 입증하였다.

침입대응 연구분야에서는 최신 해킹기법으로 활용되고 있는 봇넷을 탐지하고 대응할 수 있는 기술을 국내에서 처음으로 개발한 점과 침입패턴을 자동생성하고 정형화함으로써 시뮬레이션할 수 있는 원천기술 확보한 점을 중요 연구 연구성과로 들 수 있다.

침입방지 연구분야에서는 IPv6 환경이나 유비쿼터스 환경에서 안전한 서비스 운영이 가능하도록 하는 인증, 인가, 비밀성/무결성 지원, 컨텍스트 지원 기능을 수행하는 보안미들웨어를 개발하였으며, 개인정보보호를 위한 프라이버시 정책언어개발과 개인정보가 저장된 DB에 대한 리눅스 커널기반의 L2/L3 수준의 보안게이트웨이 상용화가 대표적인 연구결과이다.

[그림 1]은 시스템보안연구센터에서 수행한 침입차단, 침입대응, 침입방지 연구분야의 연관성을 나타내고 있다.



〔그림 1〕 시스템보안연구센터 주요 분야 간 연관성

2.2 운영 특성

시스템보안연구센터 운영의 가장 큰 특징 중의 하나는 시스템보안분야 산업체의 실질적 연구수요 조사와 연구개발결과의 신속한 기술이전 및 상용화를 위해 '산학협력본부'를 두고 운영한 점이다. 산학협력본부는 국내 보안업체에서 필요로 하는 최신 보안기술에 대한 센터 참여교수의 멘토링 지원, 시스템보안분야의 국외 제품 및 기술개발 정보 공유, 센터 연구개발 보안기술에 대한 산업체의 평가수렴, 산업체수요 보안전문인력 정보수집 등 대학 등 연구기관들과 산업체들간이 상호협력할 수 있는 중요 기능을 수행함으로써 산학협력 중심센터인 시스템보안연구센터가 기술연구환경이 열악한 국내 정보보호업체들의 연구소로서의 역할과 기능을 담당하려 노력하였다.

이를 위해 시스템보안연구센터는 정보보호 산업체 및 연구소의 전문가를 통해 센터의 연구개발주제 및 방향에 대해 년 2회 평가회를 개최하였으며, 수요자 의견반영을 위해 산학연 디지털포렌식 워크샵 개최, 정보보호인력양성 워크샵 개최, 중소기업 멘토링 지원사업 등을 지속적으로 진행하였다.

또 다른 센터의 운영 특징은 '산학일체형 연구교육모델'을 정립하고 실천한 점이다. 이 연구교육모델은 센터 참여 구성원들의 연구경쟁력강화를 위해 참여교수들

의 연구주제선정과 연구결과를 기술적 우수성뿐만 아니라 시장부합성, 상용화 가능성 등 측면에서 외부 전문가의 평가를 정기적으로 시행하는 '참여교수 외부평가제', 보안산업체에서 요구하는 연구개발 실무경험을 갖춘 고급인력을 양성하기 위한 '산학협력 인력양성', 그리고 '연구학생 3품제도'로 구성, 운영되었다. 이 중 '연구학생 3품제도'는 연구참여 대학원생들의 연구개발능력에 대한 전문성, 팀원들 간의 협동연구능력을 평가하는 팀워크능력, 연구원의 개발일정 준수 및 개발결과의 우성을 평가하는 신뢰성을 객관적으로 평가하는 것을 목표로 운영되었다.

〔그림 2〕 산학일체형 연구교육모델

이 산학일체형 연구교육모델의 정립과 실천으로 2004년 국가균형발전위원회가 주관한 지역혁신 우수사례로 선정되어 과학기술부 장관상을 수상하였다.

Ⅲ. 주요 연구개발성과

3.1 인력 배출, 연구논문 및 특허 부문

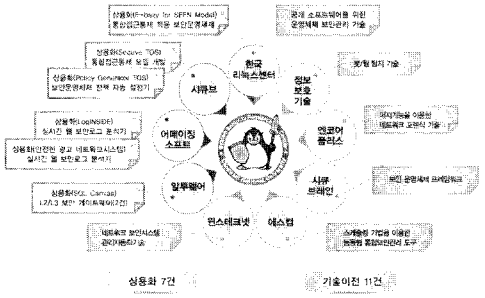
지난 8년간 시스템보안연구센터가 수행한 연구개발과제를 통해 총 200명(박사 52명, 석사 148명)의 정보보호 고급인력이 배출되었다. 배출된 인력들은 대학, 산업체, 정부기관 및 연구소에 취업하여 국내 정보보호 정책결정과 보안기술 및 제품개발에 기여하고 있다.

또한 시스템보안분야 연구를 통해 습득한 우수한 해킹방어 및 대응능력을 통해 2008년에는 국제해킹대회인 DefCon CTF 2008에서 본선 8위, 코드게이트 해킹대회 마이더스상 수상과 제5회 해킹방어대회 금상 수상, 2007년에는 국제해킹대회인 DefCon CTF 2007에서 본선 6위, KISA주관 제2회 취약점 찾기대회 대상 수상, 2006년 KISA주관 S/W 보안 취약점 찾기대회 대상 수상과 IT Festival 삼성SDS 사장상 수상, 2004년부터 2006년까지 3년 연속 해킹방어대회 대상 수상 등 국내외 해킹방어대회에서 우수한 실적을 거두었다.

2000년부터 8년간 총 158건의 SCI급 논문과 150건의 국제논문, 234건의 국내논문을 발표하였다. 또한 10건의 국내특허등록과 12건의 국내특허출원, 그리고 1건의 국제특허출원을 하였다.

3.2 기술이전 및 상용화 부문

시스템보안연구센터는 정보보안업체의 기술수요를 반영한 센터 참여교수의 연구개발 및 개발결과물에 대해 2005년부터 4년간 11건의 기술이전과 7건의 상용화를 이루어내는 등 산학협력 중심센터로서의 역할을 충실히 수행하였다.



〔그림 3〕 상용화 및 기술이전 주요 실적

상용화된 연구개발결과물 중 다양한 접근통제정책 표현언어를 개발함으로써 보안운영체제의 정책 유연성을 향상시킨 연구주제는 2007년 9월 동북아시아 공개소프트웨어 활성화 포럼의 공식 프로젝트로 채택되었으며 해당 연구결과물은 국내 보안운영체제 선도기업인 (주)시큐브사의 Secuve TOS 제품에 적용되었다. 그리고 리눅스 커널 모듈의 Layer 2/3 계층에서 패킷 분석을 통해 개인정보가 저장된 DB에 대한 접속여부를 효과적으로 판단하는 보안게이트웨이는 DB 보안 전문업체인 (주)알투웨어사의 SQLCanvas 패키지의 핵심모듈로 상용화되었다.

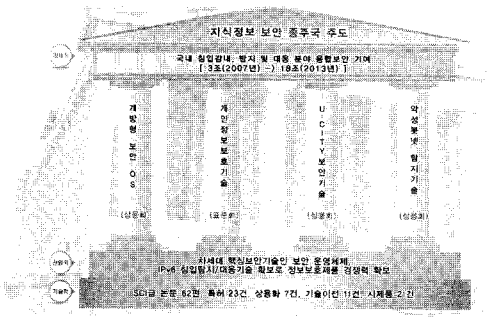
위와 같이 센터가 산업체와의 공동연구를 통해 정보

보호산업의 기술선진화와 우수인력 양성에 기여한 공로를 인정받아 2007년 산업자원부가 수여한 산업기술진흥 유공 대통령상과 한국정보보호산업협회(KISIA)로부터 제1회 산학협력공로상을 수상하기도 하였다.

3.3 사회·경제적, 기술적 효과

시스템보안연구센터가 지금까지 수행해 왔던 침입차단, 대응 및 방지를 위한 시스템분야 보안기술 개발은 지능화, 복잡화, 고도화되고 있는 다양한 해킹으로 인한 사회적 비용을 절감하고 시스템보안기술에 관한 원천기술을 확보함으로써 지식정보보안산업 종주국의 기초를 다져왔다고 판단된다. 또한 국가적으로 추진하고 있는 지식정보보안산업의 기술적 토대 구축은 물론 법률로 추진 중인 정보시스템 및 개인정보보호 정책을 뒷받침하는 기능을 담당해 왔다.

산학연 협력연구를 통해 시스템분야 원천기술인 통합보안정책모델(SEEN)을 개발하고 상용화하였으며, 최근 주요 해킹에 이용되는 봇넷 탐지 및 대응기술을 국내 최초로 개발하였다. 그리고 앞으로 그 중요성이 더해질 것으로 예상되는 개인정보보호를 위한 DB 보안게이트웨이 기술, IPv6 및 유비쿼터스 환경 보안을 위한 미들웨어를 개발함으로써 향후 증가될 것으로 예상되는 새로운 해킹기법에 대해 선제적으로 대응할 수 있게 되었다고 판단된다.



〔그림 4〕 시스템보안연구센터 연구결과의 기대효과

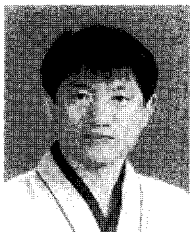
Ⅳ. 결 어

최근 지능화, 조직화, 고도화되고 있는 해킹기법들에 대해 선제적이며 효과적으로 대응하기 위한 다양한 기술적, 관리적, 제도적 장치들이 도입되고 있다. 그 중에서도 시스템보안기술은 기술의 중요성과 복잡성으로 인해 단기간 내에 자체 개발이 쉽지 않을 뿐만 아니라 정보보호 선진국으로부터 기술도입 역시 용이하지 않은 특성을 가지고 있다.

시스템보안연구센터는 기술개발이 어렵지만 정보보호를 위해 필수적인 시스템 보안기술분야의 원천기술 확보와 관련 제품의 상용화를 목표로 지난 8년간 참여교수, 대학원생, 산업체 개발인력 등이 산학협력 공동연구를 통해 노력해 왔다. 이를 통해 한중일 표준 보안운영체제에 센터가 개발한 접근통제모델이 적용되었고 560여 건의 우수한 연구논문발표와 특허 등록, 시스템보안 분야의 실용적인 기술을 갖춘 200여 명의 우수인력을 배출하였다.

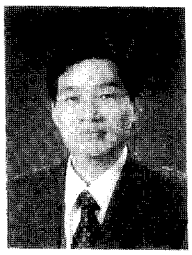
앞으로 시스템보안연구센터는 그 동안 정부지원으로 구축된 시스템보안분야 연구개발 인프라와 인적 네트워크를 활용하여 지식정보보안산업 강국으로 발돋움하는데 필수적인 운영체제보안, 개인정보보호, 봇넷탐지술, 유비쿼터스 환경의 보안기술 개발은 물론 우수한 정보보호 지역인재의 발굴과 양성 임무를 지속적으로 수행할 계획이다.

〈著者紹介〉



노 봉 남 (Bongnam Noh)
종신회원

1978년 2월: 전남대학교 수학교육과 졸업(학사)
1982년 2월: KAIST 전산학과 졸업(석사)
1994년 2월: 전북대학교 대학원 전산과 졸업(박사)
1983년~현재: 전남대학교 전자컴퓨터공학부 교수
2000년 현재: 전남대학교 시스템보안연구센터 소장
<관심분야> 컴퓨터와 네트워크 보안, 개인정보보호, 사이버사회와 윤리



이 형 효 (HyungHyo Lee)
종신회원

1987년 2월: 전남대학교 계산통계학과(학사)
1989년 2월: KAIST 전산학과 (석사)
2000년 2월: 전남대학교 대학원 전산학과(박사)
1990년~1992년: 삼보컴퓨터 기술연구소
1993년~1997년: 한국통신 연구개발원
2001년 3월~현재: 원광대학교 정보·전자상거래학부 부교수
<관심분야> 프라이버시보호, Identity 관리시스템, 보안 온톨로지, 응용보안