■ 연구과제 요약문

과제명(기간)	사회망 특성 기반 건강한 사이버 시스템 구현에 관한 연구 (2015. 5 ~ 2016. 4)
연구책임자	김 종 권 (ckim@snu.ac.kr)
개요	- 온라인 시스템은 인터넷 사용 환경의 발전과 더불어 사용자의 참여, 공유, 개방 등 웹 2.0의 핵심 가치가 투영되면서 온라인 SNS(Social Network Service)가 빠르게 성장하고 있다. 대표적인 SNS 서비스로는 페이스북, 트위터, 인스타그램이 있고 왓츠앱(WhatsApp), 라인, 카카오톡을 포함한 모바일 메신저도 온라인 SNS 성격을 가지고 있다. 다양한 온라인 시스템에서 사회망 기술을 활용하는 추세는 당분간 지속될 뿐만 아니라 확장될 것으로 예상된다. - 컴퓨터 시스템 및 인터넷 서비스는 우리 생활을 편리하고 윤택하게 하는 순기능과 함께 역기능도 가지고 있다. 사용자가 원하지 않는 문자/이메일을 불법적으로 전송하여 불쾌감을 유발하는 스팸과 이를 한 단계 발전하여 사용자에게 직접적인 손해를 가하는 피싱, 스미싱, 랜섬웨어 등으로 활용되는 사이버 공격, 추천 시스템에서의 상품 평을 고의적으로 조작하는 스팸 리뷰와 SNS를 통한 악성 루머의 확산으로 온라인 시스템의 신뢰성이 저해되는 원인이 되고 있다. 정보보안 전문가와 해커들 사이의 전쟁은 영원히 끝나지 않는 군비확장 경쟁(Arms race)과 유사하다. 예를 들어 보안 전문가들이 스팸을 탐지하기 위해 스팸어쎄신(SpamAssassin)과 같은 내용 기반(Contents Based) 필터링 기법, 스네어(SNARE)와 같은 방어 기술을 개발하면 스패머들은 방어체제를 무력화하기 위해 새로운 공격방법을 개발하고 있다. - 기존 네트웍 보안기법은 1) 텍스트의 내용 및 행동 패턴을 분석하는 기법 2) 네트워크 정보를 활용하는 기법 위주로 발전하였다. 기존 패러다임은 이메일이나 신문기사와 같은 초기 온라인 시스템을 대상으로 발전한 것으로써 상대적으로 포멀한 문서와 사용 패턴을 가정하고 있으므로 스팸SMS 탐지, 온라인 추천 시스템, 시빌(Sybil: 가짜 ID) 탐지 등 새로운 시스템 또는 응용에 적용할 경우 성능 한계를 노출한다. “사회망 특성을 이용하여 다양한 형태의 사이버 공격을 방어하고 안전하고 신뢰성 있는 온라인 시스템을 구축할 수 있을까?” 라는 근원적 질문으로 시작하여 새로운 보안 패러다임을 창출하는 패러다임 쉬프트형 연구를 제안한다. 또한 사회망 특성을 기반으로 공격 탐지/제거하는 방어적 방법을 도출함과 더불어 실제 사회의 사회망의 특성을 반영하여 건강한 사이버 시스템을 구현하는데 필요한 사회적 제도 및 방법을 도출하는 구축성(Constructive) 연구도 수행한다.
연구개발 결과	- 소셜망 특성을 활용한 효율적인 스팸 탐지 기술을 개발하였다. 스팸이란 전자 우편, 문자메시지, 전화, 인터넷 쪽지 등을 통해 불특정 다수의 사람들에게 보내는 광고성 편지 또는 메시지를 의미한다. 인터넷이 활성화 되면서 이메일에서 SMS까지 그 영역이 점점 커지고 있고 트위터나 페이스북과 같은 소셜 네트워크 서비스를 통해 더욱 확산되고 있다. 불법 도박이나 대출 등 정보 전달 뿐 아니라 메시지 속에 링크를 삽입

	하고 사용자가 접근했을 시 상대방의 개인 정보를 유출하는 피싱과 사용자의 파일 등을 강제로 암호화한 뒤 다시 풀어주는 대가로 금전을 요구하는 랜섬웨어(Ransomware)가 PC와 스마트폰에서 지속적으로 발견되고 있어 사회적으로 문제가 되고 있다. 따라서 이를 해결하는 방법으로 국내· 외 기업 및 연구기관에서 이메일이나 SMS의 내용을 토큰화 한 뒤 각 토큰에 대한 점수를 부여하고 스팸과 비스팸을 구분하는 내용 기반 스팸 필터링과 이메일의 헤더 부분에서 IP 주소를 추출하여 blacklist/whiltelist를 구축하는 네트워크 기반 스팸 필터링 기법, 어플리케이션에서 사용자들이 받은 스팸을 신고하여 이를 데이터베이스에 저장하고 이와 같은 이메일/SMS가 왔을 시 스팸으로 분류하는 크라우드소싱 기법이 연구/서비스되고 있다. 하지만 위의 방법들은 지속적인 트레이닝이 필요하고 발신자의 정보가 자주 바뀌는 경우에는 적용하기 어렵다는 단점이 있다. 본 연구팀은 이러한 문제를 해결하고자 소셜 네트워크의 특성을 이용하여 스패머와 정상 사용자들에 대한 특성이 명확하게 구분되어 효과적으로 분류한다.
활용분야 및 기대효과	**- 사이버 범죄예방에 활용** 온라인 사회망 구조 분석기반 공격자 탐지 기법은 기존 보안 기법들이 잡아내지 못했던 공격들을 원천 차단할 수 있다. 두 기법을 모두 활용할 경우 더 큰 시너지 효과를 기대할 수 있다. 해당 기술은 국내 금융사고 피해를 최소화 할 수 있으며, 해외 판로를 개척할 경우 수출 또한 가능하다. 스패머나 피싱에 대응했던 기존 기능들을 쉽게 대체할 수 있으므로 보안 시스템 비용을 획기적으로 감소시킬 수 있다. **- 보안 시스템 개발에 적용** 개인정보 보안에 대한 사회적 인식은 오래전부터 존재해 왔지만, 이를 위한 도구와 기술수준은 아직 성숙하지 못한 것이 사실이다. 최근 국내에서는 여러 금융기관과 민간기업에서 개인정보 유출 사고를 겪었으며, 이에 대한 피해는 고스란히 사용자의 몫으로 돌아가고 있다. 이 문제는 비단 국내뿐만 아니라 전 세계적으로 심각한 사회적 이슈로 떠올랐다. 미국을 비롯한 세계 각국은 개인정보 보안에 대한 법을 강화하고 보안 기술에 대한 예산편성을 늘리는 추세다. 유출된 개인정보는 온라인 사회망을 통해 걷잡을 수 없이 빠르게 퍼져나가기 때문에 추가 피해를 막기 힘든 특징이 있다. 본 연구팀의 개발 요소기술로 활용되는 Information Diffusion 및 Maximization 이론을 응용할 경우 유출이 발생해도 정보 확산 정도를 예측하여 해당 메시지 전송을 선별적으로 차단하여 개인정보 유출 확산 속도를 크게 줄일 수 있다. 따라서 사회 안전과 편익 증진에 기여할 수 있다.