情 報 保 護 學 會 誌
第22卷 第3號, 2012. 5

COP 보안기술 동향

김 태 경*

요 약

인터넷은 사회 경제적 상호작용을 위한 기본적인 인프라가 되어 사람들에게 많은 혜택을 주는 반면 여러 가지 다양한 위험들을 가져왔다. 또한 인터넷을 사용하는 어린이의 수가 증가하고, 그 연령이 더 어려지면서 어린이를 온라인상에서 보호하는 것은 중요한 이슈가 되고 있다. 본 논문에서는 온라인상에서 미성년자를 보호하기 위한 기술적인 대처 방안에 대한 분석을 수행하였다. COP의 다양한 기술들을 활용하여 어린이들을 위험으로부터 벗어나게 할 수 있으며(filtering technologies), 특정한 사이트에 어린이를 접근하지 못하게 하고(age or identity verification systems), 인터넷 상에 어린이들을 안전하게 할 수 있는 안전지대(walled garden)를 만들 수 있다. 이러한 기술적인 대처 방안들은 여러 기술들을 조합하여 사용해야 그 효과성을 높일 수 있으며, 특히 미성년자들의 개인정보 보안을 고려하여 균형적으로 사용해야 한다. 이외에도 COP에서 기술적인 대처방안의 발전적인 개발을 위해서는 보안기술 사이에 정보를 공유할 수 있는 표준이 개발되어야 하며, 보호 기술의 장점 및 기능을 파악할 수 있는 표준 성능 인자의 개발이 필요하다.

Ⅰ. 서 론

인터넷은 사회 경제적 상호작용을 위한 기본적인 인프라가 되어 사람들에게 많은 혜택을 주는 반면 여러 가지 다양한 위험들을 가져왔다. 또한 인터넷을 사용하는 어린이의 수가 증가하고, 그 연령이 더 어려지면서 어린이를 온라인상에서 보호하는 것은 중요한 이슈가 되고 있다. 인터넷의 발전과 확산은 아동들에게 온라인 교육, 게임, 음악 등 문화생활 제공, 무수한 정보에 대한 접근의 기회 등 무수한 이익을 제공해주는 한편, 다양한 역기능과 역효과들을 함께 가져오고 있다. 불법 콘텐츠의 유통, 사이버 폭력, 포르노, 온라인 게임 중독, 온라인 사기, 사이버 상 인종차별 등 온라인 세상에서 아동이 노출되어 있는 위험은 점점 더 다양하고 심각해져 가고 있어, 이에 대한 대처가 시급히 요구되고 있다. 온라인 아동보호(Child Online Protection, COP)는 네트워크로 연결된 인터넷의 특성상, 다른 사이버 이슈와 마찬가지로 온라인 아동보호 문제도 한 개별국가의 독자적 문제가 아닌 국제적 수준에서 협력하고 정책적 대응 방안이 확립되어야 한다[1].

온라인의 위험은 사회적 그리고 문화적인 요인과 인터넷에 접속할 수 있는 어린이의 능력에 따라 나라와 나라마다 다르게 나타난다[2]. 어린이들의 활동과 기술이 다양해지고 온라인 환경과 그에 따른 다양한 상호작용이 발생하면서 관련된 결과들도 다르게 나타나게 된

〔표 1〕 법률에 의해 의무적으로 수행되는 정책 조치의 예

Country	Policy measure	Complementary technical policy measure
Korea	Regulation of child-inappropriate content	Access restriction via reliance on national identity verification systems
Italy, Korea, Turkey	Regulation of prohibited and illegal content	Mandatory ISP-level filtering
United Kingdom	Online gambling prohibition	Online gambling websites are required to put age verification in place
Japan	Regulation of child-inappropriate content	Mandatory filters on mobile phones of users under 18 unless parents opt out
United States	Parental consent requirement under COPPA	E-mail from parents' e-mail account, provision of parents' credit card details, written consent form from the parent, or telephone call from parent

* 서울신학대학교 교양학부 (tkkim@stu.ac.kr)

다. 온라인 위험에 대한 어린이들의 취약점은 경험과 인식 그리고 위험한 환경을 처리하는 능력의 부족에 기인한다. 다양한 위험들의 결과는 다양하게 나타나는데, 여기에는 물리적이고 정신적인 피해도 포함되며, 경제적인 영향도 간과할 수 없다.

대부분의 나라들은 인터넷이 어린이들에게 자기표현, 교육, 학습 및 창조적인 온라인 활동에는 동의하고 있다. 또한 어린이들의 인터넷 사용은 어린이들을 다양한 위험에 직면하게 하고 있다는 것에도 의견을 같이하고 있다. 그러므로 여러 나라에서는 어린이들이 인터넷을 사용할 때 보호될 수 있도록 온라인 위험을 감소하는 다양한 정책들을 수행하고 있다[3].

본 논문에서는 COP의 활동 중 기술적 관점을 중심으로 그 현황을 살펴보고자 한다.

Ⅱ. COP 관련 보안기술

COP에서 보안기술은 종합적으로 고려되어야 하며, 하나의 기술로 어린이들의 보호에 관한 모든 문제를 해결할 수는 없다. 즉 여러 기술들을 조합하여 사용해야 효과적인 보호를 수행할 수 있다. 모든 기술 해결책들은 각기 그 성능에 제한을 가지고 있으며, 어린이 온라인 안전 방법들은 프라이버시와 사용자 정보의 보안과 조화되어 수행되어야 한다[2].

2.1 Age Verification/Identity Authentication

나이 검증 기술(Age Verification Technology)은 어른과 어린이들의 나이를 확인하는 것이며, 신원 인증(Identity Authentication)은 개인의 신원을 확인하는 것이다. 이러한 기술들의 주요 목적은 나이를 부적당한 콘텐츠에 접속하는 것을 제한하는 메커니즘으로 활용하는 것이다. 나이를 확인하기 위해 사용되는 방법은 다양한데, 여기에는 신용카드나 국가적인 ID 카드 혹은 면대면 확인 등이 포함한다. 신용카드를 사용하여 나이를 검증하는 방법은 가장 많이 설치되어 사용되는 방법이지만, 나이 검증에 대한 우회 가능성이 있어서 그 성능에 제한점을 가지고 있다. 즉 어린이가 부모의 신용카드를 사용하여 어른으로 인증되는 방법 등이 존재한다. 면대면 검증방식도 독일이나 미국에서 많이 사용되는 나이 검증 방법이지만 이 방법은 오프라인 검증 방식으로 분류되고 있다. 한국에서는 주민번호의 노출 가능성을 막기 위해 i-Pin 시스템을 사용하고 있다.

이 범주의 기술들은 다음과 같이 분류할 수 있다.

⊙ 공공 데이터베이스에서 수집한 정보와의 비교

부동산 거래, 범죄 정보, 신용 보고서 등 사적이나 공적으로 어른에 대해서 수집한 정보들을 개인에 대한 포트폴리오 데이터로 집약할 수 있다. 이러한 정보들을 이용해서 다양한 어플리케이션에서 개인에게 정확한 정보를 물어봄으로써 신원을 확인한다.

⊙ 학교나 공공기관에서 수집한 정보와의 비교

일반적으로 제 3의 기관에서는 어린이에 대한 정보를 수집하기 어렵다. 그래서 이 방법은 학교나 공공기관에서 수집한 정보를 이용하는 방식이다. 단, 학교나 공공기관에서 수집한 정보에 접근하기 위해서는 부모나 어린이의 동의가 필요하다.

Age verification/Identity authentication 기술은 개념적으로는 많이 논의되고 있지만, 그 효과성 측면에서는 도전을 받고 있다. 이는 정보의 원격 인증에 의존하는 시스템의 경우에는 잠재적인 부정확성이 존재하기 때문이다. 예를 들면, 사용자 측면에서 신원을 확인하려고 시도하는 사람이 자신의 실제 정보를 이용하는 것인지, 다른 사람의 정보를 이용하는 것인지 확인할 수 없다. 그러나 공공기록에 의존하는 시스템의 경우에는 남아있는 기록으로 인해 어른에 대한 확인을 좀 더 정확하게 수행할 수 있다. 또한 제3의 신뢰기관에 의한 검증 시스템의 경우에는 정치적 지지나 사회적 수용 등의 합의가 필요하다.

나이 검증 및 신원 확인을 위해서는 어떤 형태이든지 개인의 정보가 축적되어 비교 및 검증되어야 하는데, 이러한 개인 정보의 중앙 저장소는 개인정보보호 및 보안문제를 발생시킬 수 있는 여지가 있으므로 주의해야 한다.

2.2 Filtering/Monitoring/Auditing

필터링, 모니터링 및 감사 솔루션은 부적절한 콘텐츠에 접근하는 사용자를 차단하거나 사건이 발생한 후에 사건 기록을 문서화하는 모니터링 메커니즘을 제공한다. 이 기술은 미리 정해진 규칙에 따라 웹 콘텐츠를 동적으로 모니터링하며, 즉각적으로 적절한 접근 계층을 결정한다. 이 도구들은 소프트웨어 기반으로 사용자의 컴퓨터에 설치되며, 로그를 기록하는 기능이 구성되어

있어, 개인들이 컴퓨터에서 인터넷 활동들을 검토할 수 있도록 허용한다. 이러한 필터링, 모니터링 및 감사 도구는 인터넷 규제가 적정하게 수행될 수 있는 부모, 학교 및 기타 공공장소에서 사용되어 광범위한 성공을 거두고 있다.

필터링, 모니터링 및 감사 도구는 일반적으로 클라이언트 측 도구 및 서버 측 도구의 두 가지 범주로 나눌 수 있다.

⊙ 클라이언트 측 도구

클라이언트 측 소프트웨어는 사용자의 컴퓨터에 로컬로 설치되고, 사용자에 의해 관리되어진다. 이 도구의 효과성은 사용자의 설치, 구성, 정기적인 유지보수 및 소프트웨어의 사용에 달려있다. 특히 클라이언트 측 필터링 도구는 10년 이상 설치되어 많이 사용되고 있다. 이러한 도구들은 부모 및 보호자들에게 대체적으로 안전한 인터넷 환경을 제공하기 위한 쉬운 구현방법을 제공한다.

⊙ 서버 측 도구

콘텐츠가 사용자의 컴퓨터에 도달하기 전에 서비스 플랫폼이나 웹 사이트의 규칙에 의해 부적절한 콘텐츠가 필터링 되는 작업이 수행된다. 예를 들면, 소셜 네트워크 사이트는 사용자에 의해 생성되지만 일부 사용자들에게 부적절한 것으로 간주되는 콘텐츠를 필터링할 수 있다. 그러므로 사용자의 기호 보다는 웹사이트의 정책이 사이트에 적합한 제한 범위와 정도를 결정한다.

또한 필터링 기술은 사용자의 개인 장비나 ISP (Internet Service Provider) 계층 혹은 모바일 운영자 계층 그리고 검색 엔진 계층 등 다양한 계층에서 운영된다. 필터링은 whitelists 혹은 blacklists에 기반을 둔 기술이다. Whitelists는 사용자에게 적당하게 정리된 목록 이외의 모든 콘텐츠를 차단하는 것이고, blacklists는 사용자에게 적당하지 않다고 기록된 리스트를 제외한 모든 콘텐츠의 접속을 허용하는 것이다.

어린이들에게는 whitelist 접근이 추천되는데 이는 방대한 정보에 접근하게 하는 것보다는 안전한 환경이 어린이에게는 더 중요하기 때문이다. 그러나 나이가 점차 증가하면서 blacklist 접근방법을 사용하여 점차적으로 다양한 정보를 얻을 수 있게 해야 한다. Blacklists는 미리 정의된 분류나 실시간으로 분석하여 능동적으로 생성되는 목록에 의해 유지될 수 있다. 이러한 목록들은 콘텐츠를 생성하는 곳이나, 신뢰할 수 있는 제3의 기관에 의해 생성될 수 있다.

필터링은 정보기술과 통신기반에 걸쳐 다양한 계층에 설치될 수 있다. 그 계층으로는 네트워크 계층(e.g. Internet Service Provider network or local area networks), 서비스 계층(e.g. social network site or search engine), 최종 사용자 터미널 계층(e.g. mobile phone or computer) 등이 있다[3].

네트워크 계층 필터링은 네트워크의 모든 사용자를 위해 미리 정의된 콘텐츠에 의해 접근을 차단하는 것보다 효과적인 것으로 간주된다. 이러한 네트워크 계층 필터링은 인터넷 서비스나 전용선 제공자의 네트워크 계층이나 사용자의 로컬 영역 네트워크 계층에서 수행된다. 네트워크 계층 필터링의 범위 및 목적은 필터링이 발생하는 곳에 따라 달라진다. 네트워크 서비스 제공자의 네트워크에 설치된 필터는 현지법에 따라 불법적인 콘텐츠를 차단하는 목적으로 모든 인터넷 트래픽을 필터링한다. 몇몇의 인터넷 서비스 제공자들은 네트워크 기반의 부모 제어 방법을 제공하는데, 이는 부모의 요청에 따라 유해 콘텐츠, 특정 어플리케이션, 프로토콜 혹은 서비스를 차단한다.

콘텐츠 필터링은 서비스 계층에서 수행된다. 예를 들면, 독일이나 프랑스에서 운영되는 포탈의 검색엔진은 neo-Nazi 웹사이트의 리스트를 차단한다. 또 다른 서비스 계층 필터링으로는 서비스 제공자에 의해 개발된 whitelist 접근방법인 어린이 버전의 포탈이 있다. 이에 대한 예로서는 주니어 네이버가 있다.

최종 사용자 계층 필터링은 최종 사용자의 장비에 설치된 프로그램이나 브라우저에 설치된 플러그인 등에 의해 수행된다. 이에 대한 필터링 브라우저의 예로서 Glubble이 있는데, 인터넷에 접속하기 위해서는 브라우저에 비밀번호를 입력해야 한다.

필터링, 모니터링 및 감사 소프트웨어는 부모 및 감독을 하는 어른들에게 특정 형식의 부적당한 인터넷 콘텐츠에 사용자가 접근하는 것을 결정하고 제한하는 것을 도울 수 있는 유용한 도구이다. 비록 미성년자의 온라인 안전을 위한 완벽한 해결책은 아닐지라도 이러한 유형의 기술들은 안전한 인터넷 환경을 제공하기 위해 부모가 참여하고, 어른이 감독하고 소프트웨어 도구가 함께 작업하는 방식으로 COP의 핵심 기능의 중요한 역할을 담당할 수 있다.

부모 제어 소프트웨어는 온라인에서 어린이의 안전

을 높이기 위해 기술적인 해결책으로 가장 많이 사용되고 있는 방법이다. 기본적으로 필터링 기술에 기반을 두고 있으며, 부모 제어 소프트웨어 도구들은 콘텐츠 필터링뿐만 아니라, 웹캠이나 메신저와 같은 특정 어플리케이션을 제어하는데, 이를 통해 어린이들의 온라인 사용에 대한 내역이나 인터넷 사용의 시간제한 설정 등의 기능을 할 수 있다. 그러므로 부모 제어 소프트웨어는 콘텐츠 관련 위험을 넘어서 통신 위험과 같은 광범위한 대상을 목적으로 하고 있다[4].

최근 미국에서는 부모 제어 솔루션을 인터넷 서비스 제공자에 의해 제공되게 하거나 부모에 의해 쉽게 구매할 수 있는 다양한 방안들에 대해서 연구를 수행하고 있다. 이 기술의 가장 큰 장점으로는 콘텐츠 생산자나 네트워크 서비스 제공자들의 허락 없이 독립적으로 운영을 할 수 있다는 것이다.

2.3 Text Analysis

텍스트 기반의 분석기술은 인터넷에서 비방하거나, 괴롭히는 등의 부적절한 대화를 자동적으로 감지하도록 설계되어 있다. 이러한 기술들은 일반적으로 검사되어야 하는 대화들에서 통계적인 시그니처를 추출하고, 측정된 통계를 기반으로 대화를 분류함으로 샘플을 얻는 방식으로 작동한다. 텍스트 분석 도구는 인터넷 카페, 도서관 그리고 전체 소셜 네트워크 웹사이트에 이르기까지 설치 규모에 차이가 있다. 일부 텍스트 분석도구는 가정용 컴퓨터에 로컬로 설치되어 부모의 검사 도구로 자동분석을 수행하는 기능을 수행한다.

텍스트 분석 기술은 청소년들을 위해 온라인 안전을 제공하는 유망한 기술이지만, 아직 이 기술은 대체적으로 초기 단계에 머무르고 있다. 이러한 단점을 수용하기 위해서는 자동화된 텍스트 분석기술의 구현이 필요하다. 이 기술은 부모들이 인터넷에서 어린이들을 보호하기 위한 필터링, 모니터링 그리고 감사활동을 보완하기 위해서 사용할 수 있다. 이 기술은 사용자에게 명확한 보안기준을 제공하는 학교 및 다른 공공의 기관들에서 전반적인 보안 프로그램의 일부분으로 이 도구를 설치한 후, 기술의 유용성을 검증한 후에 효과적으로 사용할 수 있다.

2.4 Biometrics

바이오인식은 개인의 생리적 특성이나 얼굴 이미지 등의 고유의 특성을 이용하여 개인의 나이를 확인하는 방법이다. 이러한 바이오인식 기술은 물리적(지문, 홍채 또는 DNA 등) 또는 행동적(타이핑 스타일 등) 특성을 기반으로 개인을 식별한다. 바이오인식의 중요한 기술 개발은 많이 진전되어 있으며, 제한된 상업적인 사이트에 설치되어 있다. 이러한 도구들은 컴퓨터를 사용한 하드웨어 기반의 장치를 이용하여 특정 바이오인식 정보를 받아 전송한다. 한 예로, 개인의 손에서 뼈 밀도 분석을 이용하여 개인의 연령 그룹을 결정하는 장치가 시도되고 있다. 또 다른 도구는 얼굴인식 기술을 이용해 특정한 개인을 식별하고, 이를 공개된 성범죄자 데이터베이스와 비교하는 작업을 수행한다.

이외의 다른 기술로는 사용자의 타이핑 방법이나 패턴분석을 통해 특정 사용자를 인식하는 방법을 사용하고 있다. 각 인스턴스에서 정보는 하드웨어나 소프트웨어 도구에 의해 수집되고, 특정한 서비스를 사용하여 사용자의 적합성을 결정하기 위해 이용된다. 그러나 현재는 정확성 및 검출 속도 그리고 감독에 대한 필요성 등의 다양한 이유로 인해 광범위한 사용에 어려움이 있다.

이러한 기술 이외에도 많은 국가의 산업에서는 어린이들을 위한 장비들을 제공하고 있다. 특히 휴대 전화 단말기 같은 경우에는 어린이들을 위해서 인터넷 접속이나 블루투스 등의 기능을 비활성화 시켜 어린이를 보호한다. 일본에서 모바일 회사가 어린이 단말기를 판매할 경우, 기본적으로 인터넷 접속이 제한되도록 설정되어 있다. 미국의 모바일 운영자는 부모의 제어를 허용하는데 인터넷 접속을 차단하거나 웹 콘텐츠를 차단하고, 원하지 않는 전화나 텍스트 메시지를 차단할 수 있다.

Ⅲ. COP 보안 기술 가이드라인

COP 보안기술 적용에 대한 기술적 가이드라인은 다음과 같이 정리할 수 있다[2].

3.1 보안기술은 온라인상에서 미성년자의 보호를 위한 역할을 하지만 유일한 해결책은 아니다.

비록 인터넷이 감독이 되는 운동장이나 다른 공공의 장소처럼 쉽게 모니터링 되진 않지만, 교육적인 측면이나 지식 및 상업에 접근하는 측면에서 큰 이점을 제공하고 사회와 접촉하는 상호작용을 하게 한다. 그리므로

미성년자들의 다양한 온라인 활동을 가능하게 하면서 효과적으로 보호하기 위해서는 아동 및 부모에 대한 교육, 주기적인 부모의 참여나 책임 있는 어른의 참여, 지속적으로 증가하는 기업의 책임 및 보안과 관련된 중요 소프트웨어 도구들이 통합적으로 고려되어야 한다.

3.2 가장 효과적인 기술 해결책은 여러 기술들을 조합하여 사용해야 한다.

많은 COP 보안 기술들은 온라인상에서 미성년자의 안전을 위한 전체적인 분야를 고려하기 보다는 특정한 분야에 대한 보안 해결책을 제시하였다. 이는 미성년자의 온라인 보호가 다각적인 문제이기 때문이다. 그러므로 여러 보완적인 보안기술들을 적용함으로 미성년자의 온라인 활동에 대한 안전성의 효과성을 높일 수 있다.

3.3 모든 보안기술들은 제한사항이 있다.

인터넷 영역에서 미성년자의 안전을 보장하기 위한 많은 기술들이 존재하고 있으나, 이를 회피하기 위한 다양한 기술들도 존재하고 있다. 그러므로 각 기술들에 대한 제한사항을 고려하여, 보안에 취약한 부분이 발생하지 않도록 효과적인 보안 도구들의 사용을 고려해야 한다.

3.4 청소년 온라인 안전 도구들은 미성년자의 정보 특히 개인정보의 안전을 고려해야 한다.

거의 모든 기술적인 도구들은 개인정보의 잠재적인 노출 가능성이 있다. 그러므로 축적된 사용자 정보가 안전하도록 적절한 개인정보보호 및 보안대책을 수립하는 것이 중요하다. 게다가 취약성이 있거나 신뢰하지 못하는 제3의 기관에게 개인정보를 제공할 때에는 개인정보가 노출되지 않도록 보안을 강화할 수 있는 기술적인 대처 및 비용을 고려해서 개인정보의 노출 폐해를 차단해야 한다.

Ⅳ. COP 보안 기술의 고려사항

COP 기술의 효과적인 개발 및 사용을 위해서는 보안기술 사이에 정보공유를 위한 표준이 필요하다. 현재는 미성년자의 온라인 보안을 향상시키는데 관심이 있는 사용자, 사이트 그리고 제3의 기관들 사이에 자발적으로 정보를 공유할 수 있는 개방형 표준이 없는 상태이다. 그러므로 COP를 위한 보안기술의 개방형 정보공유 표준은 특정한 서버나 클라이언트 쪽 기술을 고려하지 않고 사용자의 프라이버시를 보호하는 목적으로 벤더의 참여하에 개발되어야 한다. 이러한 정보공유 표준의 개발은 미성년자의 온라인상의 안전을 향상시킬 수 있는 획기적인 기회를 제공할 수 있을 것이다.

또한, 청소년 보안 솔루션을 위한 표준 성능 인자의 개발이 필요하다. 청소년들을 온라인상에서 보호할 수 있는 다양한 기술들이 존재하지만, 이러한 기술들의 성능을 검증할 수 있는 표준 성능 인자들은 없는 상태이다. 이러한 표준 성능 인자들의 개발은 여러 보안기술들에 대한 상대적인 장점과 단점을 평가하는데 도움을 줄 수 있다. 이러한 표준 성능 인자들을 개발하는 것은 많은 노력이 필요하지만, 미성년자의 온라인 보호를 향상시키는 데 중요한 역할을 수행할 것이다.

Ⅴ. 결 론

하나의 온라인 보안기술이 미성년자가 직면하고 있는 다양한 온라인 안전문제를 해결할 수는 없지만, 각 기술들은 각기 다른 장점을 가지고 있으며, 몇몇의 기술들은 미성년자의 보호에 큰 도움을 줄 수 있다. 게다가 COP 보호 기술들은 미성년자가 문제가 있는 콘텐츠에 접근하거나 성적 강요, 온라인 괴롭힘 등을 제한하는 중요한 기능을 수행한다. 그러나 기술만으로는 직접적으로 주어진 문제의 근본적인 해결책을 제시할 수 없다. 그러므로 기술을 포함한 다각적인 측면에서 미성년자의 보호에 대한 사회의 전반적인 협조가 필요하다.

이외에도 COP 보안기술이 효과적으로 사용되기 위해서는 모든 사용자의 컴퓨터에 보안 소프트웨어가 설치될 수 있도록 적정한 가격 설정에 대한 고려가 필요하다.

참고문헌

[1] 박민정, "온라인 아동보호를 위한 ITU의 활동", 방송통신정책 제22권 6호, 2010년 4월.

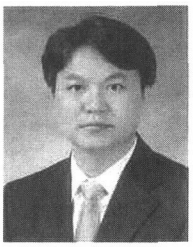
[2] ISTTF (Internet Safety Technical Task Force) (2008), "Enhancing Child Safety and Online

Technologies": Final Report of the ISTTF to the Multi-State Working Group on Social Networking of State Attorney Generals of the United States. Cambridge, MA: Berkman Center for Internet and Society, Harvard University.

[3] OECD (2011), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD Publishing.

[4] http://ec.europa.eu/information_society/activities/sip/index_en.htm.

〈著者紹介〉



김 태 경 (Kim Tae Kyung)
정회원
1997년 2월: 단국대학교 수학교육과 졸업
2001년 8월: 성균관대학교 정보통신공학과 공학석사
2005년 8월: 성균관대학교 전기전자및컴퓨터공학과 공학박사
2006년 3월~2008년 2월: 서일대학 정보전자과 교수
2008년 3월~현재: 서울신학대학교 교양학부 교수
<관심분야> 네트워크보안, USN, 클라우드컴퓨팅