情 報 保 護 學 會 誌
第21卷 第1號, 2011. 2

ID 관리 기술과 표준화 동향

정 영 곤*, 장 기 헌*, 이 상 래*, 장 재 훈*, 진 승 헌**, 염 흥 열*

요 약

인터넷이 활발히 보급되고 활성화 되면서 그로 인하여 사용자는 많은 정보를 다루게 되고 수많은 자신의 정보를 기억하고 활용하기는 쉽지 않다. 이렇게 수많은 자신의 정보를 효율적이고 안전하게 관리하는 ID관리 중요성과 필요성이 대두되었다. 본 고에서는 국내외적으로 개발된 ID관리 기술들을 조사하고 분석하고 ID관리와 관련된 표준화의 동향을 국내외 표준화 기구를 대상으로 살펴본다. 또한 요즘 들어 이슈화되고 있는 클라우드 컴퓨팅과 ID관리 기술을 융합하는 기술과 표준화의 동향을 알아본다.

Ⅰ. 서 론

사용자의 인증정보를 비롯하여 신상정보, 선호도, 개인의 특징과 같은 ID의 생성부터 변경, 유통, 폐기 등과 같은 정보를 온라인 환경에서 안전하고 효율적으로 관리하는 ID관리 기술이 필요하다. 요즘날 인터넷의 확산으로 많은 웹사이트 들이 생겨났다. 그에따라 사용자는 많은 웹사이트마다 아이디와 패스워드를 등록하고 개인 신상정보를 입력해야하고 또한 기억해야 한다. 초기에는 사용자가 스스로 관리가 가능하였지만 현재는 감당할 수 없을 정도로 양이 늘어났다. 또한 ID와 패스워드 뿐만 아니라 사용자의 신용정보, 개인의 신상 정보 등의 관리가 필요하다. 사용자가 상품을 구매하여 지불을 할 때에 필요한 금융정보의 양 또한 방대하다. 거래하고 있는 계좌를 비롯하여 보안카드, 할인정보 등을 사용자가 모두 외우고 효율적으로 사용하기가 쉽지 않다. ID관리는 사용자의 편의와 안전하고 효율적으로 자신의 정보를 활용하기위한 기술이다.

국내에서 ID관리 기술의 표준화 전략으로 2008년부터 국제 표준의 선도를 위한 기반을 구축하여 2013년까지 국제 표준의 선도를 목표로 활발히 진행되고 있고 현재에는 진입단계에 있다.

본 고에서는 국내외의 ID 관리 기술의 동향을 보이고 국내외 표준화 기관에서 추진중인 ID관리 관련 표준화의 동향을 살펴본다. 마지막으로 클라우드 컴퓨팅과 ID 관리의 융합 표준화 전략을 본다.

Ⅱ. ID관리와 표준화의 필요성

인터넷 상에서의 ID 도용 및 개인정보유출 문제는 이전부터 존재해 왔다. 하지만 최근 들어서 사용자의 정보를 취급하는 기업에서 정보의 대량 유출과 같은 사건이 발생하고 있다. 2008년 국내 최대 인터넷 쇼핑몰 중 한 곳에서 1,000만 여명의회원 정보가 해커에 의해 유출되어 회원의 개인정보와 금융정보가 노출된 후 스팸 및 보이스 피싱 등 2차 공격에 악용된 사고나 유명 통신업체에서 600만 명의 회원정보가 불법 거래되는 사건이 발생하였다. 개인정보 유출에 대한 문제의 심각성이 일반인에게 알려지면서 안전한 ID관리가 사회적인 문제로 인식되고 있는 상황이다.

이렇게 온라인 환경의 편리함으로 인하여 점차 커져가고 있는 ID만큼 온라인상에서 사용하는 ID관리의 불편함과 개인정보 오남용으로 인한 피해를 줄이기 위한 기술의 개발이 필요한다. 또한 국내 ID관리 표준을 국제 표준으로 추진하여 국내에 경제적, 기술적으로 이득을 가져다 준다. 경제적으로는 국내 기술의 수출증대와 국제시장의 진출로 인한 국내 기업의 수익 증대를 가져오고 기술적으로는 ID관리의 핵심기술을 조기 확보하고 빠르게 공유하여 훌륭한 기술로 안전한 ID관리를 할 수 있다.

* 순천향대학교 정보보호학과 ({ygjung,canonst12,isr3104,pure,hyyoum}@sch.ac.kr)
** 한국전자통신연구원 (jinsh@etri.re.kr)

Ⅲ. 국내외 ID 관리 기술

3.1 국내 ID관리 기술

3.1.1 i-PIN

i-PIN제도의 도입배경은 특정한 정보를 가진 정보제공자가 서비스를 제공하고자 할 때 회원가입을 유도하며 취득하는 회원의 주요 정보(주민등록 번호, 카드번호 등)를 획득함으로부터 시작이 되었다. 이렇게 획득한 회원의 주민등록번호(개인정보)는 순수한 회원관리로 운영되면 문제가 없지만, 악의적인 목적으로 이용이 된다면 그 피해는 고스란히 회원으로 가입한 개인에게 돌아가게 된다.

대한민국 정부는 재발하는 이러한 문제점을 해소하고자 정보통신부와 행정안전부를 주관으로 주민등록번호 대체 수단인 i-PIN이 도입하게 되었다. i-PIN은 행정안전부 i-PIN 발급 사이트에서 본인실명 및 정보를 입력 후 발급받게 되며 정보제공자 즉, 자의에 의해 가입하게 되는 대한민국 국적의 웹사이트에 회원 가입 시 주민등록번호 대신 i-PIN 을 입력함으로써 정부가 본인을 인증해 주는 서비스 시스템이다[9].

3.1.2 전자지갑

전자ID지갑은 일상생활에서 사용하는 지갑처럼 인터넷 상에서 사용되는 사이버 지갑이다. 전자ID지갑은 사용자는 자신의 주소, 전화번호 등과 같은 개인정보, 계정 정보 등과 같은 인증 정보와 신용카드 등과 같은 지불정보들로 구성된 Identity 정보를 보관한다. 사용자가 인터넷 웹 사이트에서 서비스를 받으면서 웹 사이트가 사용자 인증, 개인정보, 결제 정보 등을 요구하면, 자신의 전자 ID 지갑에서 필요한 정보를 확인하여 웹 사이트에 제공하는 방식으로 운용된다[1].

최근에는 전자 지급 수단과 전자 화폐가 대중적인 결제 수단으로 자리잡아가고 있다. 이동통신인 모바일과 결제 시스템의 결합이나 대중교통 결제수단인 티머니가 대표인 예이다. 또한 근거리 무선 통신 기술(NFC)는 근거리 접촉만으로 데이터 통신이 가능하다는 큰 장점을 가지고 있으며, 아직 초기 단계이지만 금융 분야를 시작으로 유통, 가전까지 응용분야가 확대 된다면 휴대폰이 전자지급 시장의 중심 축으로 떠오를 전망이며, 일상에도 큰 변화를 가져다 줄것이다.

SK C&C의 경우 TSM 솔루션과 전자지갑 솔루션 기술을 제공하고, FC는 금융기관 및 유통점 등에 대한 마케팅 및 서비스 운영을 전담하기로 되어 있으며, SK Telecom에서도 스마트폰을 이용한 모바일 결제 수단이 활성화 되면서 이를 마케팅 수단으로도 사용하고 있다.

3.2 국외 ID관리 기술

3.2.1 Microsoft CardSpace

MS와 IBM, Novell 등이 웹 개발자, 애플리케이션 개발자들과 공동으로 표준화된 '메타시스템(metasystem)'을 개발하였다. 정보 카드(Information Cards)로 명명된 이 시스템은 서로 상이한 ID 시스템이 상호 연동하여 작동하도록 하고, 이용자들이 보다 친숙하게 디지털 ID를 이용하는데 목표를 두고 있다. Information Card의 구축은 윈도 카드스페이스(Windows CardSpace)로 명명된 프로젝트로 진행되고 있으며 .NET 프레임워크 3.0에 기반을 둔다.

이 기술을 통해 이용자들은 접속하고자 하는 웹사이트나 온라인 서비스에 특정 정보를 포함하는 카드를 생성하여 제시할 수 잇으며, 웹사이트나 서비스에서 요구하는 정보만을 제공하도록 개별적인 카드를 소유할 수 있다[3][4].

3.2.2 OpenID

OpenID는 사용자 중심의 Identity를 위한 분산형 공개 표준 기술로 인터넷 상에서 URL(Uniform Resource Identifier)를 이용하여 사용자 자신을 식별하게 해주는 인증 프로토콜이다. OpenID에서 사용자 소유의 URL은 자신을 식별하기 위한 ID이며, 인증에 필요한 패스워드(또는 인증서)는 사용자가 직접 운영하는 서버나 서비스 제공자에 의해 보관된다.

오픈 ID의 가장 큰 장점은 ID 관리의 편의성 향상과 더불어 사용자 중심의 인증 방식으로 인해 사용자가 자신의 개인 정보를 Identity 제공자를 통해 제어할 수 있는 수단을 제공한다는 것이다. OpenID의 보안 이슈 중 가장 큰 문제는 피싱으로 인한 개인정보 유출 방지와 신뢰된 인증 시스템 구현이다.

OpenID는 초기부터 다른 ID 기술에 비해 복잡성이

제거되었고, 이는 최근 사용자들의 참여가 확대되는 웹 2.0 환경에 쉽게 적용될 수 있는 장점으로 작용한다 [4][10].

3.2.3 IAF

IAF(Identity Assurance Framework)는 Liberty Alliance의 IAEG(Identity Assurance Expert Group)가 관리하며, 2008년 6월 1.1 버전 스펙을 공개하였다. 이 스펙은 미국의 e-Authentication 전략 프레임워크를 기반으로 Common Organization 서비스 평가, Identity Proofing 서비스 평가, Credential Management 서비스 평가 항목을 4단계 보증 레벨에 따라 구분하였다. 또한 IAF의 구축단계에서 조직의 순응도, identity proofing 서비스, 인증서 강도, 인증서 관리 서비스 등을 평가하는 체계를 다룬 Service Assessment Criteria(SAC) 드래프트 버전을 2009년 6월 릴리즈하였다.

3.2.4 Kantara Initiative

이니셔티브는 2009년 6월 Concordia, DataPortability Project, Information Card Foundation, Internet Society, Liberty Alliance, OpenLiberty.org, XDI.org의 7개 단체와 ID관리 기업 45 곳이 참여하며, 상호운용이 가능한 ID관리 솔루션을 전세계에 보급시키는 것을 목적으로 한다. 공개 표준에 근거하여 사용자의 편의성, 보안, 프라이버시 보호에 초점을 맞추며, 이를 통해 IAF, ID-WSF, Information Card, OAuth, OpenID, SAML 2.0, WS-*, XACML, XDI 등의 표준을 조합한 솔루션이 개발될 예정이다[2].

3.3 기술 전망

ID관리 분야는 SAML, Liberty Alliance와 같은 기업 위주의 ID관리 기술과, CardSpace, OpenID 등의 사용자 중심의 ID관리 기술로 양분되어 진행되고 있다. 기업 위주의 ID관리 기술은 법률이나 규제를 만족하면서 조직 내외부의 ID 정보를 안전하게 공유하는 방법을 다루고 있으며, 개별 기술보다는 실제 적용을 고려한 프레임워크 관점을 지향하고 있다. 이에 따라 SAML을 기반으로 하는 Liberty Alliance의 IAF, IGF, e-Authentication 전략 등이 업계를 중심으로 개발 및 적용될 전망이다. 사용자 중심의 ID관리 기술은 급격하게 진행되고 있으며, 관련 표준 및 사용자들의 증가 추세가 뚜렷하다. OpenID의 경우, 초기에는 신뢰를 고려하지 않은 블로그 수준의 인증에만 사용될 것으로 예상되어 파급력이 미미했으나 최근에는 whiltelist나 PAPE 같은 신뢰 기반의 연결을 고려하고 있다. 또한 google, yahoo, microsoft, myspace, facebook, daum 등의 메이저 업체가 OpenID를 지원하고 있으며 OpenID 수는 5억여 개에 달한다. 마지막으로 CardSpace의 경우, Identity Selector를 개발하는 여러 프로젝트들의 상호호환성을 만족하는 기준으로 ISIP(Identity Selector Interoperability Profile)가 사용되고 있으며, 여러 기업들이 ISIP를 준용하는 솔루션을 개발하고 상호운용성 시험을 통과한다. 현재는 CardSpace의 도입이 지체되고 있지만, 향후 id/pw 기반의 인증 체계를 근본적으로 변화시키는 대안이 될 것이다.

Ⅳ. 표준화 동향

4.1 국내 표준화 동향

4.1.1 TTA

TTA에서는 TC5/PG502(개인정보보호 및 ID관리 프로젝트그룹)에서 ID관리 표준화를 주도적으로 진행하고 있다. 2009년을 시작으로 ID관리 표준을 개발하고 있다. TTA에서 ID관리와 관련하여 제정된 표준은 아래의 내용과 같다[5].

- 사용자 중심 ID 관리 서비스의 안전성 검증 항목 : 본 표준에서는 사용자 중심 ID 관리 서비스에서 프라이버시 침해 유형을 분석하고, 이를 통해하여 서비스 주체별 보안 요구사항을 제시하였다. 또한, 사용자 중심 ID관리 서비스의 안전성을 평가하기 위한 안전성 검증 항목도 함께 제시하였다.
- 스마트 디바이스에서의 모바일 아이덴터티 관리를 위한 요구사항 : 본 표준은 스마트 디바이스에서의 모바일 아이덴티티의 보안 및 프라이버시 보호, 모바일 아이덴티티의 안전하고 편리한 사용 및 서비스 상호 연동, 모바일 아이덴티티에 기반한 고부가 서비스 개발을 위한 모바일 아이덴티티 관리 요구사항을 정의하였다.
- 아이덴터티 관리 기본 용어 정의 : 이 표준은 아이

덴티티 관리에서 사용되는 주요 용어에 대한 정의를 제공한다. 가장 기본적으로 중요하고 공통적으로 많이 사용되는 아이덴티티 관리 용어들로 구성되어있다. 몇가지 중요한 용어에 대한 배경지식이 부록에 수록되어있다.

- 모바일 아이덴터티 관리 프레임워크 : 본 표준은 모바일 단말에서 사용되는 모바일 아이덴티티의 보안 및 프라이버시 보호, 모바일 아이덴티티의 안전하고 편리한 사용 및 서비스 상호 연동, 모바일 아이덴티티에 기반한 고부가 서비스 개발을 제공하는 퍼스널 모바일 아이덴티티 관리 프레임워크를 정의한다.

4.1.2 표준화 추진체계 및 전략

국내표준은 산업계, 학계, 연구기관으로 구성된 디지털 ID관리 포럼 등을 통하여 산업체의 요구사항을 수렴한다. 그 후에 ETRI, KISA, 정보보호산업체에서 국내표준 초안은 개발하고 TTA를 통하여 정보통신 단체표준으로 개발을 추진한다. 그래서 ID관리분야에 상당부분 국내 표준화를 이루었고 몇몇 아이템은 현재 활발히 진행중에 있다. TTA에 개발되고 제정된 국내 표준을 기반으로 국제표준을 선도하기 위하여 ITU-T, ISO/IEC JTC1에 국내 표준 전문가들이 활발히 참여하여 국내에서 개발된 ID관리 및 개인정보보호 기술에 대한 국제 표준화를 수행한다[5].

4.2 국외 표준화 동향

4.2.1 ITU-T

2006년 12월부터 2007년 9월까지 진행된 Focus Group IdM에서는 IdM과 관련된 활동 중인 표준화기구, 포럼 및 컨소시엄 목록을 정리하고 일반적인 IdM 프레임워크 요구사항 도출을 위한 사용 사례 시나리오를 작성하였다. 그 외에 ID관리를 다룬 스터디 그룹이 있는데 Q.15/13(NGN Security)에서는 NGN(Next Generation Network) 환경에서 보안 요구사항 권고안을 확정하였고 인증, AAA, 보안 메커니즘, NGN 인증서, IdM 보안 등에 관한 권고 초안을 개발중에 있다[6].

ITU-T에서 ID관리의 표준 개발을 직접적으로 담당하고 있는 곳은 SG17의 Q10이다. 한국의 ETRI에서 제안하여 현재 진행중인 기고문으로는 X.idmsg - Security guidelines for identity management systems 라는 제목으로 어떻게 IdM 시스템이 NGN(Next Generation Network)나 사이버 환경에서 보안 아이덴터티 서비스를 전개하고 제공되어야 하는지 가이드라인을 제공한다. 이번 2010년 12월에 제네바에서 열린 ITU-T SG17회의에서 새로운 워크 아이템으로서 baseline capabilities and mechanisms of IdM for mobile applications and environment라는 제목으로 모바일 어플리케이션과 환경의 의미를 정의하고 모바일 어플리케이션과 환경을 위한 IdM의 기본 역량을 정의하는 등의 내용이 포함되어 있다.

4.2.2 ISO/IEC

ISO/IEC에서는 JTC1 SC27 WG5에서 ID관리 프레임워크 국제 표준 개발을 진행중에 있고, ID관리 프레임워크 개발을 위한 먼저 이루어져야 할 작업으로 ID 온톨로지 정의를 들고 있다. ID 온톨로지는 실제적인 ID관리에 필요한 용어와 개념 공유를 위해 필수적이다, 이 ID 온톨로지는 ID관리 프레임워크 이용자에게 ID관리와 관련된 일관된 시각을 제공하여 서로 상이하거나 연관된 목적을 가진 서로 다른 사용자와의 협력을 가능하게 하는 중요한 역할을 담당하고 있다. 또한 ID 개념, ID, 식별(identification) 및 식별자(identifier), ID 생명주기, ID 인증, 정보사회에서 ID관리, 정보기술과 ID관리, 정보보안과 ID관리 등 포괄적인 ID관리에 대한 표준 개발을 진행하고 있다[8].

4.2.3 OASIS

OASIS에서 제정한 ID 관련 표준들로 SAML(Security Assertion Markup Language), XACML(Extensible Access Control Markup Language), SPML (Service Provisioning Markup Language), XRI(Extensible Resource Identifier), WS-Security(Web Service Security) 등이 있다. 이중 ID관리와 가장 밀접한 관계에 있는 SAML 표준에서는 사용자, 자원, 서비스 프로비저닝 정보교환을 위한 XML 기반 프레임워크를 정의하고 있으며 XRI 기반 프레임워크를 정의하고 있다. 이러한 OASIS의 SAML 표준은 ITU-T에 제안되어 X.1141로 표준화가 되었다[7]. 또한 ID 관리와 관련된

표준으로 XRI는 인터넷 규모의 URI기반 추상화된 ID를 정의하는 명세와 XRI 데이터 공유를 위한 조율 프로토콜, 도메인 상호간에 자원 공유 등을 명세하고 있다. 이 OASIS의 XRI 표준은 한국의 TTA에서 국내표준으로 수용한 상태이다.

4.2.4 Liberty Alliance

Amex, AOL, GM, HP, Nokia, Sony, Sun 등의 약 150여기 업체로 구성되어있는 표준기구이다. Federated Identity 관리와 인터넷 SSO에 대한 표준을 제정하고 있으며 현재 SAML v2.0으로 통합되었다. ID-WSF (Web Service Framework)는 사용자가 자신의 Identity 정보를 다른 시스템에 공유할 수 있도록 해주는 웹 서비스 프레임워크를 정의하고 있다. 이 ID관리 기술을 활용하기 위해서, 인터넷 서비스 제공자인 SP(Service Provider)는 사전에 IdP(Identity Provider)와 다양한 정책에 대한 협의를 통해 CoT(Circle of Trust)를 구성해야 한다. 일반적으로 CoT는 단일 또는 소수의 IdP와 다수의SP로 구성된다[3].

V. 클라우드에서의 ID관리

5.1 OASIS

CA, IBM, MIcrosoft, Symplified, Novell, Ping Identity 등이 참가하는 OASIS IDCloud라는 그룹을 만들어 클라우드 컴퓨팅에서의 ID관리 표준화를 추진하고 있다. OASIS와 관련된 산업계는 지금 가상화와 클라우드 컴퓨팅이 컴퓨터의 역사에서 가장 중요한 정보 기반 구조의 재설계를 대표하는 것을 알고 있다. 이 새로운 IDCloud 위원회의 목적은 클라우드 컴퓨팅에 현재 존재하는 정의, 전문용어, 용어를 종합, 정리하고 identity 전개, 제공, 관리를 위한 공개 표준의 프로파일을 개발한다. 만약 현재 표준들 중에 상호운용을 이루기 위해 프로파일에 필요가 있으면, 존재하는 ID 표준들에서 Use cases, 위험평가, 위협분석에서 차이점을 연구할 것이다.

5.2 ITU-T

ITU-T SG17 Q10/17에서 ID 관리의 표준화 개발을 주도적으로 하고 있다. 클라우드 컴퓨팅의 발전은 다양한 신뢰 프레임워크를 사용하여 연합 관계와 신뢰를 연구의 필요성이 증가하고 있다. 계속적으로 클라우드 컴퓨팅으로 이동함에 따라서 ID 서비스 제공자와 그와 연관된 기업 등을 위한 보안과 프라이버시 규칙을 구성하고 신뢰 프레임워크를 정의한다. 클라우드 안에서, 신뢰 프레임워크는 보안, 프라이버시, 향상된 도입의 프로파일 기반 표준을 사용하여 ID의 공유를 위한 토대를 제공한다[6]. 2010년 12월 ITU-T SG17 회의에서 새로운 연구 아이템으로 클라우드 컴퓨팅에서의 IdM 요구사항을 제안하였다. 이 기고서는 클라우드 컴퓨팅 환경에서 ID 관리의 스켈레톤을 주고 클라우드에서 ID 관리의 연구 시작의 제안을 목적으로 한다. 또한 ITU-T SG17 Q10/17는 2010년 12월에 Identity Summit을 열어 다양한 아이덴터티 관리 분야에서 많은 전문가들이 모여 의견을 교환하였다.

VI. 결 론

지금까지 국내외 ID관리 기술과 표준화의 동향을 살펴보았다. 국내외적으로 ID관리의 중요성과 필요성을 느끼고 기술 개발은 물론 국제표준을 추진하고 있다. 안전하고 효율적인 ID관리 기술을 개발하여 표준화로의 추진이 필요하다. 국내의 기술과 표준을 국제 표준으로의 확장을 추진하여 2012년도에는 한국이 국제표준에 선도할 수 있도록 추진한다. 한국의 ID관리 국제 표준 선두를 위해 ITU-T 부의장을 중심으로 전문가들이 에디터로 참가하여 활발한 활동이 기대된다. 국내 표준의 국제 표준화로 국내 기술의 세계화와 선도를 이루어야 겠다.

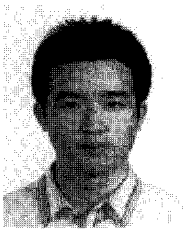
현재 이슈화 되고 있는 기술중에 하나가 클라우드 컴퓨팅이다. 이 클라우드 환경에서는 ID관리가 보안, 서비스 측면에서 중요한 역할로 대두되고 있다. 새로운 기술을 개발하기 보다는 기존의 표준을 이용하여 적용할 수 있는 방안을 연구중이다. ITU-T와 OASIS에서 개발하는 클라우드에서의 ID관리 표준화에 적극적으로 참여하여 국내 기술과 표준을 국제표준으로 추진해야 하겠다.

참고문헌

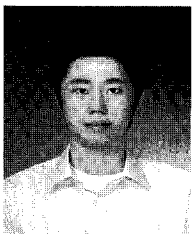
[1] 조영섭, 진승헌 "디지털 ID 관리 기술 동향 및 전망", 한국인터넷정보학회 9(3) pp14-24, 2008년 9월

[2] Kantara Initiative, "http://kantarainitiative.org/"
[3] 윤재석, 민경식, 김정희, 정보통신산업진흥원, "[IITA] 정보통신연구진흥원 학술정보 주간기술동향 1311호"
[4] 조영섭, 진승헌, 한국전자통신연구원, "[ETRI]전자통신동향분석 제22권 제3호", 2007. 6
[5] 한국정보통신기술협회, "http://www.tta.or.kr/index.jsp"
[6] ITU-T SG17, "http://www.itu.int/ITU-T/studygroups/com17/index.asp"
[7] OASIS, "http://www.oasis-open.org/home/"
[8] ISO/IEC JTC1 SG27, "http://isotc.iso.org/livelink/livelink?func=ll&objId=8916751&objAction=browse&sort=name"
[9] 안영훈, 육석예, 김진원, 김윤정, 이화영, "인터넷에선 주민번호 대신 아이핀(i-PIN)", 방송통신위원회, 한국정보보호진흥원, 2008년 9월
[10] OpenID, "http://openid.co.kr"

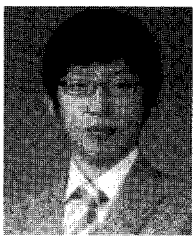
〈著者紹介〉



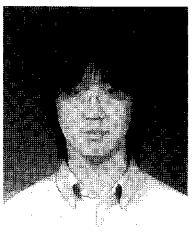
정 영 곤(Young-Gon JUNG)
학생회원
2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> IPTV 보안, ID 관리, 역추적



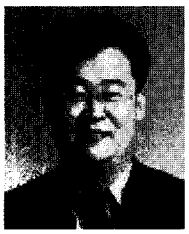
장 기 헌(Ki-hun, JANG)
학생회원
2010년 2월 : 순천향대학교 정보보호학과 졸업
2009년 4월~2010년 5월 : SK인포섹 모의해킹팀
2010년 9월~현재 순천향대학교 정보보호학과 석사과정
<관심분야> 정보보호, 스마트폰 보안, 네트워크 프로토콜



이 상 래(Sang-Rae LEE)
학생회원
2010년 2월: 순천향대학교 정보보호학과 졸업
2010년 3월: 순천향대학교 정보보호학과 석사졸업
<관심분야> 정보보호, 클라우드 컴퓨팅 보안, 역추적



장 재 훈(Jaehoon JANG)
학생회원
2009년 2월: 순천향대학교 정보보호학과 졸업
2009년 3월~현재: 순천향대학교 정보보호학과 석사과정
<관심분야> 역추적, IPTV 보안, USN 보안, 웹 보안



진 승 헌(Seung-Hun JIN)
정회원
1993년 2월 : 숭실대학교 전산학과 졸업
1995년 2월 : 숭실대학교 전산학 석사
2004년 2월 : 충남대학교 전산학 박사
1999년 ~ 현재 : 한국전자통신연구원 인증기술연구팀 팀장
<관심분야> PKI, 프라이버시, 정보보호

염 흥 열(Heung-Youl YOUM)
정회원
1981년 2월 : 한양대학교 전자공학과 학사 졸업
1983년 2월 : 한양대학교 대학원 전자공학과 석사 졸업
1990년 2월 : 한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장, 수석부회장(역), 학회장(현)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜