http://dx.doi.org/10.14400/JDC.2016.14.9.287

아이핀 보증 등급에 기반한 보증 모델

염흥열
순천향대학교 정보보호학과

A proposal of assurance model based on i-PIN assurance level

Heung-Youl Youm
Department of Information Security Engineering, SoonChunHyang Univ. Korea (Republic of)

요 약 최근 인터넷을 이용한 전자거래나 전자정부서비스가 활발히 이용되고 있다. 온라인 서비스를 이용하는 동안 다른 사람의 신원을 도용하는 문제가 빈번히 발생하고 있다. 따라서 이에 대응하기 위해서는 온라인 서비스를 이용할 때에도 높은 수준의 신원확인이 수행되어야 한다. 2006년에 국내에 도입되어 운영되고 있는 아이핀 (i-PIN, Internet-Personal Identification Number)은 인터넷 상의 신원확인번호이다[1]. 아이핀은 온라인상의 본인확인 기능을 제공하며, 아이핀 정보(연계정보, 중복가입정보)를 정보통신서비스제공자에게 제공한다. 이런 이유로 아이핀은 온라인에서 주민등록번호를 대체하는 수단으로 활용되고 있다. 본 논문에서는 국내 본인확인 수단인 아이핀의 기본 능력을 분석하고, 아이핀의 활용 및 안전성을 제고하기 위한 보증 모델의 기준을 제안한다. 그리고 제안된 아이핀 보증 모델의 안전성과 특성을 분석한다.

주제어 : 아이핀, 보증 레벨, 신원 확인, 인증, 크레덴셜 관리

Abstract The electronic transactions over the Internet are growing across the world recently. There have been a lot of identity theft incidents during these online transactions nowaday. Therefore, a high level of identity proofing shall be carried out when using online services to deal with these matter. To prevent this kind of incident, i-PIN was introduced in Korea, which is used as an Internet Personal Identification Number. The i-PIN is designated to provide an online identification of the Internet users. As such, the unique identification numbers are provided to the internet service providers. This paper is to analyze the capabilities that the i-PIN provides, to propose the assurance security model for i-PIN. Furthermore, the security analysis results are presented. The result of this paper can be applicable to improve the applicabilities of the i-PIN.

Key Words : i-PIN, assurance level, identity proofing, authentication, credential management

1. 서론

우리나라에서는 주민등록번호, 이름, 주소 등으로 구성되는 실체의 신원을 확인할 수 있는 아이덴티티 정보를 이용해 웹 사이트의 계정을 만들고 각종 온라인 서비스를 이용하고 있다. 아이덴티티 정보는 실체가 특정 도

* 본 논문은 2016년도 미래창조과학부의 지원을 받는 정보통신 방송표준개발지원사업의 연구결과로 수행되었음 (IoT 환경에서 프라이버시 보호 국제 표준화, R1027-16-1051)
Received 1 April 2016, Revised 8 May 2016
Accepted 20 September 2016, Published 28 September 2016
Corresponding Author: Heung-Youl Youm(Department of Information Security Engineering, SoonChunHyang Univ. Korea)
Email: hyyoum@sch.ac.kr

ISSN: 1738-1916

메인에서 구분될 수 있는 속성 정보의 집합으로 표현된다[2]. 온라인에서 전자 거래와 전자정부 서비스를 받기 위해 이용자 본인 여부를 확인받아야 서비스를 제공받을 수 있는 경우, 아이핀은 비대면으로 본인확인 여부를 확인하고 우리나라 차원의 실체의 유일성을 보장하는 고유식별번호를 제공하고 있다.

2005년 인터넷상에서 주민등록 번호를 이용하여 본인확인을 수행하던 시기에 아이핀은 주민등록번호를 대체하는 수단으로 도입되었던 한국형 아이덴티티 관리 시스템이다. 아이핀은 인터넷 상에서 이용자 본인확인, 이용자 고유 식별정보 제공, 그리고 발급받은 아이핀 아이디와 패스워드를 이용한 추가 본인확인 기능도 제공하고 있다[3].

아이핀은 실체를 본인확인한 후 이용자의 연계정보와 중복가입정보 등으로 구성된 고유식별정보를 정보통신서비스제공자에게 제공한다. 이용자의 과거 아이핀 서비스 이용 내역이 없고 본인확인을 요구하는 웹사이트에 가입하려 하는 경우, 정보통신서비스제공자는 해당 이용자를 아이핀을 발급하는 본인확인기관으로 넘겨 비대면으로 본인확인을 수행한 후 본인확인기관으로부터 아이핀 정보를 받아 해당 이용자에게 웹사이트에 가입토록 하는 절차를 수행한다. 만약 이용자가 이미 기존 아이핀 본인확인기관의 계정을 갖고 있다면 본인확인기관에 의해 다시 본인확인을 수행하지 않고, 본인확인기관은 간단히 아이디와 패스워드, 그리고 일회용 패스워드 (OTP) [4] 등을 이용해 인증한 후 해당 정보통신서비스제공자에게 아이핀 정보를 제공한다.

아이덴티티(identity)는 주어진 문맥에서 이용자를 식별하기 위해 하나 이상의 이용자 속성정보를 요구하며, 아이덴티티 정보는 이용자와 관련되는 속성 정보의 집합으로 정의된다. 크리덴셜(credential)은 이용자의 주장을 입증하는 데 필요한 증거로 표현된 데이터로 정의된다[2].

또한 기존의 아이덴티티 관리체계를 근본적으로 수정하고자 하는 노력도 제안되고 있으며[23], 기존의 주민등록번호를 대체하는 수단에 대한 연구도 추진되어왔다[25].

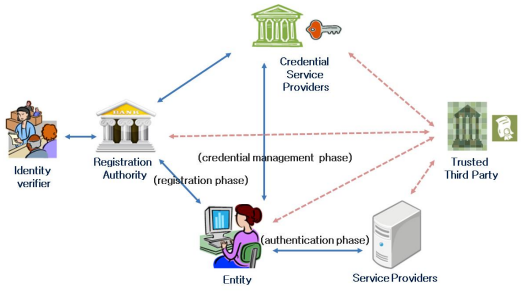
본 논문은 2장에서 연구배경과 연구내용을 제시하고, 3장에서 기존 아이핀의 보증 수준을 제시하며, 4장에서 국내 본인확인 수단인 아이핀의 개선 방향을 제시하고, 아이핀의 활용도를 넓히고 안전성을 높이기 위한 아이핀 보증 모델과 관련 기준을 제안하고, 제안된 보증 모델의 안전성을 제시한다. 제5장에서는 결론을 제시한다.

2. 배경 및 연구동향

2.1 국외 연구동향

최근 미국표준기술연구소(NIST)에서는 미국 연방정부 정보시스템에 적용 가능한 실체인증보증프레임워크를 공개했고, 국제전기통신연합-표준화부문(ITU-T) 연구반 17과 ISO/IEC JTC 1/SC 27에서는 실체 인증 보증 모델에 대한 국제 표준을 각각 채택했다.

- **NIST SP 800-63 전자인증 가이드라인[5]**: 미국의 NIST는 2011년 6월 OMB의 가이드라인(OMB M-04-04)을 보완한 전자인증 가이드라인[6]을 2011년 12월 공개했고, 2013년 9월 개정했으며, 현재는 다음 버전의 전자인증 가이드라인을 개발 중에 있다. NIST 전자인증 가이드라인은 전자인증 과정, 토큰 및 인증에 대한 위협요소, 인증 메커니즘 등의 기술적 가이드라인에 대해 기술하고 있으며 각 항목에 대한 보증 모델 등의 요구사항을 제시하고 있다.



[Fig. 1] Relying parties of entity authentication assurance framework

- **ITU-T X.1254 및 ISO/IEC 29115**: 두 국제 표준은 실체인증을 위한 실체 인증 보증프레임워크에 관한 표준이며 실체 인증 보증을 관리하기 위한 프레임워크를 제공하고 있다. ITU-T에서 X.1254 [7]를 국제 표준으로 채택하였으며(2012년

9월 7일), ISO/IEC JTC 1에서는 ISO/IEC 29115 [8]를 2013년 국제 표준으로 채택하였다. 실체인증을 위한 보증 프레임워크에서는 인증 위협을 완화하기 위한 4가지 보증 수준을 제공하고 있으며, 실체인증 보증의 단계에 대한 지침, 보증 모델 수준과 다른 인증 보증 기법과의 매핑에 대한 지침, 실체인증 프레임워크의 구성 요소, 실체 인증 관련 관리 및 조직의 고려사항, 위협 및 제어, 운영 서비스 보증 레벨 등에 대해 기술하고 있다. 또한 2016년 3월 ITU-T SG17 회의에서는 생체 인증과 인증 상승 등의 추가적인 요구를 반영하기 위해 기존의 실체인증보증프레임워크 국제표준인 X.1254의 개정 작업을 시작했다[24].

- **실체인증보증프레임워크 연구회기 (SP on EAAF):** ISO/IEC JTC 1/SC 27에서는 2015년 10월 회의에서 현재 실체인증보증 프레임워크를 개선하기 위해 연구회기를 진행 중이다[22].

2.2 아이핀 [10]

i-PIN은 온라인 환경에서 정보통신서비스제공자가 사용자를 본인 확인할 수 있는 인터넷상 개인 식별 번호이다[1]. 정보통신사업자는 i-PIN 정보를 이용하여 중복가입 여부, 생년월일, 성별 등을 확인할 수 있다. 이용자는 정보통신사업자에게 주민등록번호를 제공하지 않아도 되기 때문에 온라인 본인확인을 위한 주민등록번호의 이용을 근본적으로 방지할 수 있다. i-PIN은 2005년 10월부터 민간 본인확인기관을 통해 처음 서비스를 제공하였으며, 2009년 7월부터 이용의 편의성을 개선한 i-PIN 2.0이 발표되었다. i-PIN 2.0은 웹 사이트 간 또는 웹 사이트와 오프라인 서비스 간에 동일한 사용자임을 식별할 수 있는 연계정보 (CI: Connection Information)가 추가되어, 주민등록번호를 일차키로 이용하여 제공되던 마일리지, 사이버머니 등의 사이트 간의 연계 서비스를 i-PIN을 통해 제공받을 수 있도록 했다. 또한 정보통신사업자 내 문맥에서 사용자 중복여부 식별을 위해 중복가입정보 (DI

<Table 1> Remarks of i-PIN specification

i-pin spec	rationale	remarks
providing a unique identifier	▪ i-PIN provides a unique identifier(Internet personal identification number)that can be used in multiple domains instead of social security number	○
credential management	▪ user manages ID/password or software form of one-time password for use of I-Pin	○
attribute	▪ i-PIN provides attributes such as age, gender as well as Internet personal identification number	○
pattern information	▪ i-PIN provides pattern information such as usage history query	△
identity management	▪ i-PIN provides some ability to manage their own information to the entities	△
assurance level	▪ i-PIN provides only single assurance level of service	x
routing	▪ i-PIN helps you to find the original identity verification agencies	○
linkability	▪ i-PIN provides the same identifier which makes it possible to provide connection service between different web sites	○
security capability	▪ i-PIN exchanges related information through a secure channel	○
privacy requirement	▪ i-PIN complies with the privacy requirement required in Act on promotion of information and communications network utilization and information protection	○
audit & compliance	▪ i-PIN identity verification agencies are regularly audietd by KISA and check the requirements of Act on promotion of information and communications network utilization and information protection	○
timestamp accuracy	▪ i-PIN identity verification agencies ensure the accuracy of the timestamp	○
performance, reliability, availability	▪ i-PIN identity verification agencies carry out measures to ensure the performance, reliability, and availability	○
internationalization	▪ i-PIN does not provide other language sets except korean	x

: Duplication Information)을 제공한다. 중복가입정보는 사업자 내부에서 사용자가 무한으로 계정을 생성하는 것을 제한하는 목적으로 개발되었으며, 사용자를 식별하는 값으로도 활용할 수 있다. 또한 중복가입정보가 생성될 때, 사업자의 고유번호가 입력되기 때문에 같은 사용자라 하더라도 사업자마다 각기 다른 중복가입정보 값이 생성된다.

공공 i-PIN은 2008년 4월 행정기관이나 공공기관 웹사이트에서 본인확인을 위해 사용한 방식으로 i-PIN과 같은 방식으로 사용된다[12]. 사용자는 둘 중 하나만 있으면 모든 국내 사이트에서 본인확인을 받을 수 있다.

2015년 3월 공공 아이핀 발급과정의 소프트웨어의 취약성을 이용한 75만 건의 아이핀 불법 발급 사고가 발생해 안전성에 많은 의문이 제기되었다[13]. 행자부는 이러한 취약성을 보완하기 위한 아이핀 안전성 강화를 위한 종합대책을 발표한 바 있다[14]. 여기서는 민간 아이핀에서 사용하는 해킹방지 기능(해쉬함수 검증)과 2차 패스워드 등 추가 인증 수단을 도입하고, 부정발급이 의심되는 국내외 IP 접속 시도를 즉시 차단할 계획이라고 밝혔다.

2.3 본인확인 프레임워크

아이핀은 한국형 아이덴티티 관리시스템이다. 국제표준 ISO/IEC 29003 [15]에서 요구하는 본인확인을 위한 요구사항은 세 가지이다. 첫 번째 요구사항은 유일성 이다. 유일성이란 실체에게 유일한 식별자가 제공되는 것을 말한다. 두 번째 요구사항은 존재성이다. 존재성이란 실체가 실제로 존재하는 사용자임을 증명하는 것을 말한다. 세 번째 요구사항은 연계성이다. 연계성이란 유일성과 존재성을 증명한 실체의 정보가 실제 실체의 것인지를 증명하는 것을 말한다.

<Table 2> Requirement identity proofing assurance level (X.1254)

level	registration requirement	credential management requirement	authentication requirement
4	▪ Identity is unique within a context ▪ The entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts ▪ Proof of identity through use of identity information from multiple authoritative sources ▪ identity information verification ▪ entity witnessed in person	▪ authentication related information must be created and stored in a hardware security module.	▪ the same as level 3 ▪ e.g. ID/PW + OTP + SSL/TLS
3	▪ Identity is unique within context ▪ entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts ▪ Proof of identity through use of identity information from an authoritative source ▪ identity information verification ▪ remote or local	▪ credential should be created and saved by a regular computer, or special purpose computer.	▪ multi-factor authentication ▪ exchanges authentication information through a secure channel ▪ e.g. ID/PW + OTP + SSL/TLS
2	▪ Identity is unique within a context ▪ the entity to which the identity pertains exists objectively ▪ Proof of identity through ▪ use of identity information ▪ from an authoritative ▪ source ▪ remote or local	▪ protection measures for the stored credentials should be established.	▪ single factor authentication ▪ using cryptographic authentication protocol (password-based challenge-response protocol) ▪ carry out measures against eavesdropping attack and online brute force attack ▪ e.g. ID + Challenge-based response
1	▪ Identity is unique within ▪ a context ▪ Self-claimed or selfasserted ▪ Local or remote	▪ no requirements	▪ customized ID/password based ▪ e.g. ID/PW or MAC address

실체 인증 보증 프레임워크와 연관된 주요 이해당사자는 실체(entity), 크리덴셜 서비스 제공자(credential service provider), 등록기관(registration authority), 서비스 제공자(relying party), 신원확인 검증자, 그리고 신뢰제3자(trusted third party) 등이 존재한다[7]. 실체는 자신을 본인확인할 아이덴티티 정보를 갖는다. 실체 인증은 여러 인증 팩터(factor)에 의존한다. 실체를 인증하기 위해서 실체는 등록되어야 하고, 크리덴셜 서비스 제공자로부터 인증을 위한 크리덴셜을 발급받아야 하며 적절한 인증 프로토콜을 이용해 인증 받는다. 크리덴셜 서비스 제공자는 크리덴셜을 발행/관리하거나 크리덴셜을 생성하기 위한 하드웨어, 소프트웨어 및 관련 데이터를 발행하거나 관리한다. 개인키를 담고 있는 스마트카드는 크리덴셜 서비스 제공자에 의해 발행되는 하드웨어와 관련 데이터의 예이다. 패스워드와 바이오메트릭 정보는 크리덴셜 서비스 제공자에 의해서 관리되는 크리덴셜의 대표적인 예이다. 크리덴셜이 디지털 서명 정보라면, 크리덴셜 서비스 제공자는 공개키 인증서 (public-key certificate) 를 발행한다. 각 실체는 하나 이상의 크리덴셜을 발행받거나 크리덴셜을 생성하기 위한 여러 수단을 발행해야 한다. 크리덴셜과 크리덴셜을 생성하기 위한 수단은 성공적으로 등록 과정을 완성한 이후에 실체에게 발행된다. 등록기관은 실체의 신원확인을 크리덴셜 서비스 제공자에게 보증한다. 크리덴셜 서비스 제공자는 실체의 등록 과정을 수행하는 등록기관을 신뢰한다. 등록기관은 실체의 신원확인 검증과 신원확인정보의 검증을 수행한다. 각 실체는 하나 이상의 식별자를 갖는다.

2.4 본인확인시스템 기본 역량

국제 표준 ITU-T X.1250 [16]에서 규정하고 있는 아이덴티티 관리 시스템이 가져야 할 기본 역량은 다음과 같다.

- 고유 식별자 제공: 아이덴티티 관리 시스템은 식별자를 제공한다. 식별자의 예는 이메일 주소 등이다.
- 크리덴셜 관리: 인증을 위해 요구되는 인증정보인 크리덴셜을 제공한다.
- 속성 정보 제공: 실제 주소 등의 정적 속성 정보를

<Table 3> Assurance level evaluation of i-PIN registration phase

identity verification method of i-PIN	Identification	Identification point	level
▪ identity verification using SMS text, remote	▪ identity verification using deriver's license or ID card ▪ verify the existence of the entity ▪ verify the uniqueness using Social Security number ▪ identity usage in other contexts	▪ At phone dealer shop when user create a new mobile phone	▪ level 2
▪ identity verification using certificate, remote	▪ identity verification using deriver's license or ID card ▪ verify the existence of the entity ▪ verify the uniqueness using Social Security number ▪ identity usage in other contexts	▪ At bank which is a indirect registration authority in PKI system	▪ level 2
▪ identity verification using card details, remote	▪ identity verification using deriver's license or ID card ▪ verify the existence of the entity ▪ verify the uniqueness using Social Security number ▪ identity usage in other contexts	▪ At banks or credit card companies when user makes a new credit card	▪ level 2
▪ face-to-face authentication ▪ Using ID card	▪ identity verification using deriver's license or ID card ▪ verify the existence of the entity ▪ verify the uniqueness using Social Security number ▪ identity usage in other contexts	▪ f a c e - t o - f a c e authentication	▪ level 2

관리한다. 속성정보 발견 및 조회 기능을 제공한다.

- 패턴 정보 제공: 명성 정보와 거래 정보와 같은 관찰되거나 발견된 아이덴티티 정보를 관리한다.
- 아이덴티티 정보 관리: 인가된 실체에 의한 아이덴티티 정보 관리 능력, 아이덴티티 정보 전출입 능력, 정보의 질에 관한 정보 제공 능력, 위임 능력, 아이덴티티 정보 관리 능력 등의 데이터 관리 능력을 제공한다.
- 보증 등급 정보 제공: 실체 보증 등급의 표시 기능 및 이를 위한 상호 인증 프로토콜, 관련 메커니즘에 관한 능력을 제공한다.
- 발견: 아이덴티티 발견 제공자에게 아이덴티티 자원을 발견하기 위한 프로토콜을 제공한다.
- 상호 연동 및 중계: 연계 기반 상호 연동 능력과 중계 기반의 능력을 제공한다. 연계기반 상호 연동은 직접적인 정보를 연계하며, 중계 기반 능력은 아이덴티티 정보를 중계한다.
- 보안: 안전한 거래, 부인방지, 안전한 발견, 거래정보의 감사, 거래 분석에 기반해 도용에 대응하거나 탐지하는 능력을 제공한다.
- 개인정보 보호: 목적 외 수집, 처리, 정확도 유지, 최소 수집, 목적 외 이용 금지, 유효기간이 경과한 정보의 폐기 등의 개인정보보호 능력을 제공한다.
- 감사 및 법 준수: 보안 로그 모니터링, 개인정보의 보호, 적정할 통지 등의 감사 및 법 준수 요구사항을 만족한다.
- 타임스탬프 정확성: 정확한 타임스탬프를 제공한다.
- 성능, 신뢰성, 가용성: 아이덴티티 정보의 성능, 신뢰성, 가용성 목표를 만족하기 위한 네트워크 능력을 제공한다.
- 국제화: 다양한 언어와 문자 셋을 지원하는 국제화 능력을 제공한다.

2.5 아이핀 역량 만족 평가 분석

2.4 절에서 제시된 기본 역량을 근거로 아이핀 역량의 만족 여부에 대한 평가는 <Table 1>과 같다. 분석결과, 보증 등급의 제공과 국제화 요구사항을 만족하지 못하고 있다. 따라서 보증 등급의 기능을 탑재할 필요성이 제기되며, 본 논문은 이러한 동기에서 시작되었다.

3. 아이핀 보증 모델 분석

3.1 아이핀 문제점 및 개선 고려사항

<Table 4> Assurance level evaluation of i-PIN credential management phase

credential method of i-PIN	credential management	level
▪ single-factor authentication based on ID/password which user presents(knowledge based) ▪ Using cryptographic channel during authentication information exchange	▪ ID + password + cryptographic channel	▪ level 2

<Table 5> Assurance level evaluation of i-PIN authentication phase

identity verification method of i-PIN	identity verification method	level
▪ single-factor authentication based on ID/password which user presents(knowledge based) ▪ Using cryptographic channel during authentication information exchange	▪ ID + password + cryptographic channel	▪ level 2 (single-factor authentication + protection from eavesdropping attack) ▪ level 3 (ID/PW + OTP)

<Table 6> i-PIN assurance level 1's criteria

level	registration requirement	credential management requirement	authentication requirement
1	▪ not applicable (checks only uniqueness)	▪ none	▪ none

한국형 아이덴티티 관리 체계인 아이핀은 다음과 같은 문제점을 갖고 있다.

- 아이핀은 하나의 일관적 보증 등급만을 제공하고 있어 여러 다양한 보증 등급을 요구하는 영역에 적용될 수 없다. 따라서 다양한 보증 등급을 갖는 본인확인 체계로 변화되어야 한다.
- 아이핀이 공공, 금융, 웹 서비스, 전자거래, 의료, 에너지 등 다양한 영역에 이용되기 위한 영역별 식별자를 발행할 수 없다. 또한 영역에서도 위험 평가에 근거한 보증 등급을 제공하지 못하고 있다. 이는 아이핀 정보에 영역 코드를 넣어서 적용 가능하다.

한국형 아이디관리 체계를 개선하기 위해서 다음의 사항이 고려되어야 한다.

- 현재의 주민등록번호에는 생년월일, 성별, 출생지 등의 개인정보를 포함하고 있어서 주민등록번호가 국민의 식별 번호로 이용되는 경우 근본적으로 국민의 프라이버시를 침해할 소지가 있다. 따라서 아이핀 정보가 영역별 고유식별번호로 사용할 수 있어야 한다.
- 아이핀이 다양한 영역의 본인확인 및 영역별 식별자 역할을 수행하기 위해서는 인증의 실패로 인한 피해 정도가 다르게 됨을 의미한다. 따라서 아이핀은 다양한 영역의 고유 식별자 역할을 하기 위해서는 국제 표준에 근거한 등급화된 아이덴티티 관리 체계로 진화되어야 한다.
- 아이핀의 등급은 위험 평가 요인을 고려해 결정되어야 한다. 위험 평가 요인은 실체의 지위나 명성 손상, 금전적 손실 및 법적 의무사항 위반, 형법 또는 민법의 위반, 개인 안전 위해, 민감 정보의 비인가 유출, 조직의 피해 등이다. 인증 실패로 인한 위험의 크기는 작음, 보통, 심각, 높음 등으로 평가되어야 한다. 예를 들어, 인증의 실패로 인해 민감 정보의 비인가된 유출 위험이 크다면 보증 등급 4를 설정해야 하고, 인증의 실패로 인해 개인 안전이 심각한 영향을 미치고, 민감정보가 유출되는 경우, 보증 등급 3으로 설정되어야 한다. 또한, 개인 안전과 무관하나, 민감한 정보의 유출이 우려되는 경우 보증 등급 2로 설정되어야 하며, 개인안전과 민감한 정보 유출과 무관하나 이용자에게 불편함을 초래하는 경우, 보증 등급 1으로 설정되어야 한다.

<Table 7> i-PIN assurance level 2's criteria

level	registration requirement		credential management requirement	authentication requirement
2	objective	▪ Identity is unique within a context ▪ entity to which the identity pertains exists objectively ▪ Proof of identity through use of identity information from an authoritative source or corroborative source ▪ local or remote	▪ when creating password, use at least 3 kinds of character and 8 bit long ▪ share credential to authenticate server or register the image that only one can know ▪ identity verification agencies and trusted parties should use pre-shared security channel ▪ use SSL security channel between the user and trusted parties ▪ If necessary, establish security measures for stored credential to authenticate server ▪ Server blocks unauthorized access via the access control and the user credential management such as a password in an encrypted form	▪ perform server authentication using special video at the registration process ▪ single-factor authentication ▪ between the user and the trusted authority, protect authentication information through a secure channel or use challenge - response protocol instead of sending plaintext of password ▪ carry out measures against eavesdropping attack and online brute force attack ▪ Keylogging protection program installation ▪ Account is locked when more than three times ▪ e,g, ID + challenge based response
	method	▪ remote authentication using certificate, credit card details, SMS text ▪ but, when issuing certificate, credit card, mobile phone, use ID card to perform a uniqueness, existence and identity proof		

3.2 본인확인체계 보증 기준

이용자의 본인확인 보증 프레임워크는 X.1254 [7]에서 제시된 바와 같이 세 과정으로 구성되어야 한다. 첫 번째 과정은 인증에 필요한 크리덴셜을 획득하기 전에 실체의 신원을 확인하는 등록과정, 두 번째 과정은 등록과정에서 발급받은 크리덴셜을 관리하는 단계, 세 번째 과정은 실체 인증 단계이다. 실체인증보증 프레임워크는 4 단계 보증 등급으로 구성되며, 각 단계에 대해 각 보증 등급의 다른 기준을 정의하고 있다. 각 단계마다 기준은 <Table 2>와 같다.

3.3 아이핀 보증 모델 분석

본 절에서는 3.2 절에서 제시된 보증 기준을 근거로 현재 아이핀의 등록과정 <Table 3>, 크리덴셜 관리단계 <Table 4>, 인증 단계별 보증 수준 <Table 5>의 보증 등급을 평가한다. 평가 결과, 등록 과정은 등급 2에 해당하며, 크리덴셜 관리 과정도 등급 2에 해당하며, 인증 단계도 등급 2에 해당한다. 따라서 현재 아이핀의 보증 등급은 인증의 실패로 인해 심각한 피해가 발생하는 응용에 적용되어야 하는 등급 3과 등급 4로 동작하는 응용에는 적용될 수 없는 단점이 있다.

3.4 아이핀 분석을 위한 보안 위협

아이덴티티 관리 시스템은 등록 단계, 크리덴셜 관리 단계, 그리고 인증 단계에서 발생 가능한 위협에 적절히 대응할 수 있는 통제를 제공해야 한다[7]. 등록 단계에서 위협은 다음과 같다.

- 위장(impersonation): 실체가 다른 실체의 신원 정보를 이용해 불법적으로 본인확인을 받는 위협

크리덴셜 관리 단계에서 발생 가능한 위협에 대응하는 통제를 제공해야 한다.

- 크리덴셜 생성 시 간섭: 등록 프로세스에서 크리덴셜 생성 프로세스로 정보가 전달될 때 공격자가 이를 변경하는 것
- 크리덴셜 생성/비인가된 생성: 공격자가 크리덴셜 서비스 제공자로부터 허구의 다른 실체에 대한 크리덴셜을 생성하는 것
- 크리덴셜 발행/유출: 공격자가 크리덴셜 서비스제공자에서 실체로 크리덴셜이 전달될 때 이를 복사하는 것
- 크리덴셜 활성화/비인가된 소유: 공격자가 다른 실체의 크리덴셜을 획득해, 정당한 실체로 위장해 크리덴셜 서비스 제공자에게 해당 크리덴셜을 활성화하게 하는 것

<Table 8> i-PIN assurance level 3's criteria

level	registration requirement		credential management requirement	authentication requirement
3	objective	▪ Identity is unique within a context ▪ Identity exists ▪ Proof of identity through use of identity information from an authoritative source ▪ identity is used in other contexts ▪ proof of identity information ▪ local or remote	▪ Create and save a public key certificate related credential from a regular computer, or special purpose computer using software token ▪ During enrolment process, gives OTP token to the user ▪ share credential to authenticate server or register the image that only one can know ▪ identity verification agencies and trusted parties should use pre-shared security channel ▪ use SSL security channel between the user and trusted parties ▪ If necessary, establish security measures for stored credential to authenticate server ▪ server encrypts and manages user credential(e.g. password) then blocks unauthorized access using access control	▪ perform two-way authentication ▪ Use multi-factor authentication scheme using ID / PW + public key certificate-based signature or OTP through a secure channel ▪ Authentication via all credentials through a secure channel ▪ Keylogging protection program installation ▪ Account is locked when more than three times password mismatch ▪ e.g. ID/PW + OTP + SSL/TLS
	method	▪ remote authentication using certificate, credit card details, SMS text ▪ but, when issuing certificate, credit card, mobile phone, use ID card to perform a uniqueness, existence and identity proof ▪ then verify the authenticity of identity information		

- 크리덴셜 활성화/비가용성: 크리덴셜과 연관된 실체가 정상적인 위치에 존재하지 않아 크리덴셜서비스제공자에게 적절하게 인증되지 못하는 경우와, 크리덴셜의 전달이 지연되어 정해진 시간 내에 활성화되지 않은 것
- 크리덴셜 저장/유출: 공격자가 시스템 파일로 저장된 크리덴셜에 접근해 크리덴셜을 유출하는 것
- 크리덴셜 저장/간섭: 크리덴셜과 이름을를 매핑하는 파일이 변조되어, 기존 크리덴셜이 공격자가 접근 되는 크리덴셜로 변경되는 것
- 크리덴셜 저장/복사: 공격자가 저장된 크리덴셜을 복사해 크리덴셜의 복사본을 만드는 것
- 크리덴셜 저장/실체에 의한 유출: 실체가 공개된 장소에 자신의 사용자명과 패스워드를 적어 두어 다른 사람이 이를 접근하게 하는 것
- 크리덴셜 폐지/지연된 폐지: 크리덴셜 폐지 정보가 늦게 배포되어 그 사이에 폐지된 크리덴셜이 이용되는 것
- 크리덴셜 폐지/임무 해제 후 재사용: 직원이 퇴사했음에도 불구하고 해당 계정이 삭제되지 않아 그 직원의 계정이 비인가된 사용자에 의해 이용되는 것
- 크리덴셜 갱신/유출: 크리덴셜이 갱신되어 크리덴셜 서비스 제공자에서 실체로 전달될 때 공격자가 이를 복사하여 유출하는 것
- 크리덴셜 갱신/간섭: 실체에 의해 생성된 새 크리덴셜이 실체에서 제공자로 전달될 때 변경되는 것
- 크리덴셜 갱신/비인가된 갱신: 공격자가 보안성이 약한 크리덴셜 갱신 프로토콜을 이용해 현재 크리덴셜의 유효기간을 연장하는 것
- 크리덴셜 기록보관/부인: 실체가 크리덴셜을 이용했다는 사실을 부인하기 위해 합법적인 크리덴셜을 잘못된 크리덴셜이라고 주장하는 것

인증 단계에서 발생 가능한 위협을 대응할 수 있는 통제를 제공해야 한다.

- 일반 위협: 키 스토록 로거[17], 사회공학[18], 이용자 오류 등과 같은 일반적 특성을 갖는 위협.
- 온라인 추측: 공격자가 모든 가능한 크리덴셜 값을 추측해 반복적으로 로그온을 시도하는 것.
- 오프라인 추측: 이 공격은 서비스 제공자가 실체의 패스워드를 해쉬해 보관하는 경우 적용된다.

<Table 9> i-PIN assurance level 4's criteria

level	registration requirement		credential management requirement	authentication requirement
4	objective	▪ Identity is unique within a context ▪ Identity exists ▪ Proof of identity through use of identity information from an authoritative source and corroborative source ▪ identity is used in other contexts ▪ identity information verification from authoritative source and corroborative source, face-to-face	▪ using a hardware security module, authentication related credentials are generated and the private key is stored ▪ challenge response information are generated by a hardware security module ▪ share credential to authenticate server or register the image that only one can know ▪ identity verification agencies and trusted parties should use pre-shared security channel ▪ use SSL security channel between the user and trusted parties ▪ Hardware security modules should be uniquely identified by the identification number and saved in a safe place ▪ perform bio-authentication when using hardware security module ▪ in case of face-to-face identification, hardware security modules are delivered ▪ Server blocking unauthorized access via the access control the user credential management such as a password in an encrypted form in	▪ perform two-way authentication ▪ calculate authentication information using the private key stored on the hardware security module ▪ using challenge-response method through security channel + send OTP value through cryptographic security channel ▪ Keylogging protection program installation ▪ Account is locked when more than three times ▪ e.g. ID/PW + OTP + SSL/TLS or ID/PW + signature with nonce sent from trusted entity + SSP/TLS
	method	▪ face-to-face authentication using ID card and deriver's license ▪ verify identity information authenticity by ID card authenticity verification service provided by the ministry		

<Table 10> Evaluation of the proposed I-PIN assurance model

Phase	Threats	level 2	level 3	level 4
registration	Impersonation	△*	○	○
credential management	CredentialCreation: Tampering	○	○	○
	CredentialCreation: UnauthorizedCreation	○	○	○
	CredentialActivation: Unauthorized Possession	○	○	○
	CredentialActivation: Unavailability	○	○	○
	CredentialStorage: Disclosure, Tampering, Duplication, DisclosureByEntity	○	○	○
	CredentialRevocation: DelayedRevocation, UseAfterDecommissioning	○	○	○
	CredentialRenewal: Disclosure, Tampering,UnauthorizedRenewal	○	○	○
	CredentialRecordkeeping: Repudiation	○	○	○
authentication	OnlineGuessing	○	○	○
	OfflineGuessing	○	○	○
	Phishing	○	○	○
	ReplayAttack	○	○	○
	SessionHijack	○	○	○
	ManInTheMiddle	○	○	○
	CredentialTheft	△	△	○
	SpoofingAndMasquerading	△(low level)	○	○
	Keylogging	○	○	○
	MemoryHacking	×†	△‡	○

공격자는 특정 실체의 해쉬 된 패스워드 값을 획득한 후, 가능한 모든 패스워드의 집합을 모아둔 사전(dictionary)을 이용해, 사전 안에 있는 각 패스워드를 해쉬한 결과와 데이터베이스에 저장된 해쉬 결과가 일치하는 것을 확인해서 일치된 경우 실체의 패스워드로 간주하는 것.

- 피싱[19]: 공격자가 특정 실체를 유인해 가짜 서비스제공자에게 패스워드나 개인정보를 입력하게 해서 이 정보를 이용해서 해당 실체를 위장하게 하는 경우이다. 대표적인 예는 공격자가 특정 실체에게 메일을 보내 사기의 웹 사이트로 유도해서 이 웹 사이트에 패스워드를 입력하게 만들어 탈취해 가는 것.
- 도청: 공격자가 인증 처리 과정을 수동적으로 도청해 다음 인증 세션에 해당 실체로 위장하기 위해 정보를 탈취하는 것.
- 재생공격: 공격자가 이전 인증 처리에서 획득한 정보를 재생해 해당 실체로 인증되도록 하는 것.
- 세션 하이재킹: 공격자가 이미 인증이 완료된 실체와 검증자의 세션을 중간에 가로채는 것. 공격자가 인증 쿠키를 도청하거나 예측할 수 있다면 실체와 검증자 사이에 이미 인증된 세션을 가로챌 수 있다.
- 중간자 공격[20]: 공격자가 실체와 검증자 사이에 존재해서 인증 메시지를 변경해서 실체에게는 검증자로 보이게 하고, 검증자에게는 실체로 보이게 하는 것
- 크리덴셜 도난: 공격자가 크리덴셜을 생성하거나 포함하고 있는 디바이스를 훔치는 경우이다. 대표적으로 OTP 토큰을 훔치는 것이 있다.
- 스푸핑 및 가장[21]: 공격자가 다른 실체인척 가장하는 공격이다. 이 공격의 목적은 다른 실체가 할 수 있는 행위를 수행하기 위함이다. 이의 대표적인 예는 고무로 만든 위조 지문을 이용하는 것이 있다.
- 키로그 공격: 키보드를 통해 사용자가 입력하는 정보를 원격의 해커에게 전달하는 공격
- 메모리 해킹: 사용자의 컴퓨터가 해커에 장악되어 메모리상 모든 데이터가 변조될 수 있는 공격.

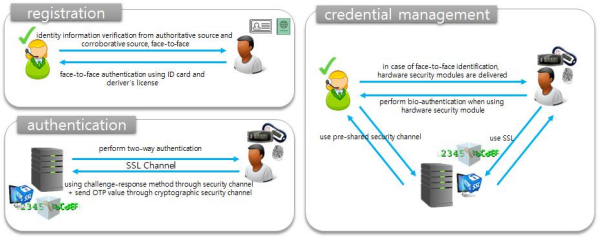
*주민등록증 위조시 가능
† 하드웨어 보안 토큰 부재시
‡ 하드웨어 보안 토큰 부재시

4. 아이핀 보증 모델 제안

4.1 아이핀 보증 모델 제안

본 장에서는 <Table 2>에 제시된 기준에 의거해 아이핀 보증 등급 모델을 제안한다. 보증 등급은 등급 1, 보증

등급 2, 보증 등급 3, 보증 등급 4로 구성된다. 아이핀 보증 등급 1은 <Table 6> 과 같이 아이핀에서는 제공될 수 없는 등급이다. 이는 아이핀은 본인확인을 요구하지만, 등급 1은 이용자 본인확인 없이 유일성만을 만족하는 등급이기 때문이다. [Table 7>은 제안하는 등급 2의 보증 모델이다. <Table 8>은 제안하는 등급 3 보증 모델이다. <Table 9>는 제안하는 등급 4 보증 모델이다. 아이핀 보증등급 모델은 등록단계, 그 후에 인증 정보 생성을 위한 크리덴셜 관리 단계, 마지막으로 자신이 정당한 본인임을 증명하는 인증 단계로 구성된다. 아이핀 발급을 위해서 등록단계는 아이핀 발급기관으로부터 신원확인을 받는 과정이며, 본인 인증을 위해 아이핀을 이용하는 과정이 인증단계에 해당하며, 아이핀 정보를 안전하게 관리하는 단계가 크리덴셜 관리 단계에 해당한다. 아이핀 사용자를 등록하고자 할 때 사용자 신원을 검증하는 신원확인 과정은 현재는 SMS 인증만을 통하여 인증을 수행하고 있으나 등급 4 보증 모델의 경우, 추가적인 신원확인 과정과 함께 하드웨어 토큰도 발행되어야 하며, 인증 과정에서도 하드웨어 기반으로 인증이 수행되어야 한다. [Fig. 2]는 제안하는 등급 4 보증 모델의 흐름도이다.



[Fig. 2] i-PIN assurance level 4's criteria

4.2 제안된 아이핀 보증 모델 안전성 평가

4.1 절에서 제안된 아이핀 보증 모델의 등록 단계, 크리덴셜 관리 단계, 그리고 인증 단계에서 발생 가능한 주요 위협에 대한 제안된 보증 모델의 안전성 평가 결과는 <Table 10>과 같다.

5. 결론

온라인 전자 거래가 활발해짐에 따라 온라인상의 본인확인이 매우 중요하다. 아이핀은 본인확인에 더해 유일성을 제공하기 위한 고유 식별자를 제공하는 보안 인프라이다. 본 논문에서는 한국형 온라인 본인확인 체계인 아이핀의 국제표준에 근거한 보증 수준을 평가했다. 아이핀의 국제 보증 등급 2에 해당해, 등급 3 또는 4를 요구하는 응용에 적용이 불가함을 확인했다. 따라서 아이핀의 활용도를 높이기 위해 국제표준인 X.1254에서 제시된 기준을 이용해 아이핀의 보증 등급 모델을 제안하고, 이에 따른 등급 기준을 제시했다. 또한 제시된 아이핀 등급 모델의 안전성을 제시했다. 본 논문의 결과는 아이핀을 포함한 국내 아이덴티티 관리체계의 개선 시에 널리 활용될 수 있을 것으로 기대하며, 실증적인 시나리오를 통한 연구 또한 차기 연구로 추가적으로 수행할 것이다.

ACKNOWLEDGMENTS

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP)(Development of International Standards for Privacy Protection in the IoT environments, R1027-16-1051)

REFERENCES

[1] KCS.KO-12.0054, "Service model and functional capabilities of the internet-Personal Identification Number Service", Sep, 2012

[2] "Recommendation ITU-T X.1252, Baseline identity management terms and definitions", April, 2010

[3] KCS.KO-12.0054, "Service model and functional capabilities of the internet-Personal Identification Number Service", Sep, 2012

[4] Soniya B. Milmile, Amol k. Boke, "Review Paper on real time password authentication system for ATM," IJAICT Volume 1, Issue 7, November 2014

[5] NIST Announces the Release of Special Publication (SP) 800-63-2, Electronic Authentication Guideline September 4, 2013

[6] OMB Memorandum M-04-04, E-Authentication

Guidance for Federal agencies, December 16, 2003.
[7] ITU-T X.1254 , Entity authentication assurance framework, September, 2012.
[8] ISO/IEC 29115, Information technology -- Security techniques -- Entity authentication assurance framework, 2013.
[9] KCS.KO-12.0170, Connecting Information for internet-Personal Identification Number Service, 2012
[10] KCS.KO-12.0038, Duplicated Joining Verification Information for internet-Personal Identification Number Service, 2012
[11] KISA i-PIN, http://i-pin.kisa.or.kr/kor/main.jsp
[12] Ministry of the Interior government personal identification number, http://www.g-pin.go.kr/
[13] The Kyunghyang Shinmun, "750,000 illegal issuance of I-pin.... government apologies in 8 days," http://news.khan.co.kr/kh_news/ khan_art_view.html?artid=201503100907371&code=940100, 2015.3.10.
[1] MOPAS, 「Countermeasures to prevent Illegal issuance of I-pin」, http://www.korea.kr/policy/pressReleaseView.do?newsId=156042425&call_from=extlink 2015.3.25.
[14] ISO/IEC CD 29003, Information technology -- Security techniques -- Identity proofing, 2016.4.
[15] Recommendation ITU-T X.1250 (2009), Baseline capabilities for enhanced global identity management and interoperability, September, 2009.
[16] Wikipedia, Keystroke logging, https://en.wikipedia.org/wiki/Keystroke_logging
[17] Whatis.com, social engineering, http://searchsecurity.techtarget.com/definition/social-engineering
[18] Cisco Phishing Overview, http://www.cisco.com/c/en/us/products/security/email-security-appliance/phishing_index.html
[19] Wikipedia, Man-in-the-middle attack, https://en.wikipedia.org/wiki/Man-in-the-middle_attack
[20] Juniper, IP Spoof Attack Prevention Overview, https://www.juniper.net/techpubs/en_US/idp5.0/topics/concept/intrusion-detection-prevention-ip-spoof-attack-prevention-overview.html
[21] ISO/IEC JTC 1/SC 27/WG 5 N235, Call for contributions to SC 27/WG 5 Study Period on entity authentication assurance framework (EAAF), 2015-11-12
[22] H.Y. YOUM, "need to change Online idetity verification system," DigitalTimes, http://www.dt.co.kr/contents.html?article_no=2015101302102251607002, 2015.10.
[23] Abbie Barbie, Heung Youl Youm, Proposal of NWI: X.1254rev Entity authentication assurance framework, ITU-T SG17 TD-2568 (Rev.1), 2016.03
[2] MOPAS, Alternative research on Social Security Number Usage by sector, SCH IACF, 2012.12.
[24] K.H, PARK, "A study of the scenario for improvement of NPKI system" Vol.8, No.4, pp.59-71, Dec 2010
[25] H.N. ZOO, "Data Protection and Privacy over the Internet: Towards Development of an International Standard", Vol.11, No.4, pp.57-69, Apr,2013
[26] B.H. KIM, "Analysis of Standard Security Technology for Security of the Network", Vol.13, No.12, pp.193-202, Dec 2015
[27] S.B. KIM, "A study on the Efficient e-Commerce Policies under the Smart Phone Environment", Vol.10, No.1, pp.125-133, Feb 2012
[28] Y.S, Choo, "Design The User Authentication Frame work Using u-helath System", Vol.13, No.5, pp.219-226, May 2015
[29] Keun-Ho Lee, "Analysis of Threats Factor in IT Convergence Security", Journal of the Korea Convergence Society, Vol. 1, No. 1, pp. 49-55, 2010.
[30] Jun-Young Go, Keun-Ho Lee, "SNS disclosure of personal information in M2M environment threats and countermeasures", Journal of the Korea Convergence Society, Vol. 5, No. 1, pp. 29-34, 2014.

염 흥 열(Youm, Heung Youl)

- 1981년 2월 : 한양대학교 전자공학과 학사 졸업
- 1983년 8월 : 한양대학교 대학원 전자공학과 석사 졸업
- 1990년 2월 : 한양대학교 전자공학과 박사 졸업
- 1982년 12월 ~ 1990년 9월 : 한국전자통신연구소 선임연구원
- 1990년 9월 ~ 현재 : 순천향대학교 정보보호학과 정교수
- 1997년 3월 ~ 2000년 3월 : 순천향대학교 산학연컨소시엄센터 소장
- 1997년 3월 ~ 현재 : 한국정보보호학회 총무이사, 국외학술이사, 교육이사, 학회지 편집위원회 위원장, 논문지 편집위원 위원장, 부회장, 수석부회장(역, 2010), 학회장(역, 2011), 명예회장
- 2005년 1월 ~ 2008년 12월 : ITU-T SG17 Q9 Rapporteur (역)
- 2006년 11월 ~ 2009년 2월 : 정보통신연구진흥원 정보보호 PM
- 2009년 2월 ~ 현재 : ITU-T SG17 부의장/SG17 WP2 의장
- 2015년 12월 : 한국정보보호학회 정보보호 대상
- 관심분야 : 인터넷보안, IoT 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜
- E-Mail : hyyoum@sch.ac.kr