Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.3, Jun. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.3.579

스마트폰 전자금융서비스에서의 인증과정에 관한 연구(앱카드를 중심으로)

김 한 우,† 이 근 영, 임 종 인, 권 헌 영‡
고려대학교 정보보호대학원

A Study on Authentication Process in Smartphone Electronic Financial Services

Hanwoo Kim,† Keun Young Lee, Jong In Lim, Hun Yeong Kwon‡
Graduate School of Information Security, Korea University

요 약

′14.5월 앱카드는 스미싱 기법과 전화번호 취득불가 취약점으로 명의도용사고를 당하였고, 그 후 카드사들은 해당 취약점을 보완하기 위해 인증수단을 추가 도입하는 등 보완하여 운영해 오고 있다. 하지만, 인증 적용환경, 목적 및 인증수단에 대한 분석이 부족하여 기존 사고에서 나타난 취약점 및 리스크수준을 낮추지 못하고 있다. 본 연구는 전자금융서비스 중 앱카드의 인증과정을 美NIST의 인증가이드라인을 적용하여 분석하고, 문제점을 파악하여 개선방향을 제안하고자 한다. 본 연구에서 분석한 방식은 앱카드외에도 인증수단의 분석에 전반적으로 적용할 수 있어 활용가치가 높을 것이다.

ABSTRACT

In May 2014, AppCard(Which is a smartphone application designed to register and use a credit card in a mobile phone by credit card company.) was attacked by smshing and a vulnerability which could not obtainable phone number. After that, credit card companies have supplemented and operated by introducing additional authentication methods to supplement the vulnerability. However, The analysis of the authentication environments, purposes and methods is not enough to lower the level of vulnerability and risk from existing accidents.

This study analyzes the authentication process of the AppCard in the electronic financial service by applying the NIST's authentication guidelines, identifies the problems and suggests improvement directions. The method analyzed in this study can be applied to the analysis of the authentication method in addition to the application card, so that it will be highly utilized.

Keywords: authentication, appcard, identity proofing, electronic financial services

I. 서 론

한국의 모바일전자금융서비스는 1999년 11월 SMS방식 모바일뱅킹으로 시작된 이후 2003년 금융칩기반 모바일뱅킹을 거쳐[1], 2009년 Apple社의 iPhone 한국 출시이후 스마트폰 기반 서비스로 진화하여 왔다. 그 중 모바일 신용카드서비스는 홈페이지를 대신하여 정보제공 및 신청을 할 수 있는 모바일앱/웹, 카드번호 등을 서비스업자에게 미리 등록한 후 사용하는 간편결제, 휴대폰에 카드를 발급(등록)해서 사용하는 모바일카드로 대별할 수 있으며, 모바일카드는 휴대폰 USIM에 카드를 직접 발급하는 USIM방식과 발급된 카드를 스마트폰앱에 등록하여

Received(04. 25. 2018), Accepted(05. 14. 2018)
† 주저자, hanuri95@korea.ac.kr
‡ 교신저자, khy0@korea.ac.kr(Corresponding author)

사용하는 앱카드방식으로 나누어볼 수 있다.

이러한 모바일전자금융서비스가 효력을 갖기위해서는 "본인의 이용"이 전제되어야하는데, 이를 위해서 "인증"이 매우 중요한 이슈가 될 것이다.

본 논문은 모바일전자금융서비스를 위해서 사용되는 "인증"이슈에 대해 2014년 발생한 앱카드 도용사고의 원인 및 현실태 분석을 통하여 살펴보고 그에 따른 문제점 및 개선방안에 대해 논해보고자 한다.

II. 이론적 배경

2.1 인증

2.1.1 언어적 관점에서의 인증

국립국어원 표준국어대사전에 따르면 한국어에서 "인증(認證)"은 "어떠한 문서나 행위가 정당한 절차로 이루어졌다는 것을 공적 기관이 증명함"으로 certification 개념을, "입증(立證)"이 "어떤 증거 따위를 내세워 증명함"이라는 뜻으로 authentication의 개념으로 뜻이 명확히 구분되어 있으나, 정보통신 분야에서는 "인증"이 "다중 사용자 컴퓨터 시스템 또는 망 운용 시스템에서, 시스템이 단말 작동 개시(log-on) 정보를 확인하는 보안 절차"[2], 개인, 조직 등이 누구인지 또는 사물 등이 무엇인지를 확인하는 절차[3]. 즉, authentication의 개념으로 사용되고 있어, 용어사용상의 혼란이 있으며, 본 논문에서 인증은 "입증(authentication)"을 의미한다.

2.1.2 법·제도적 관점에서의 인증

국내법에서 "입증"에 해당하는 "인증"의 의미는 전자서명법1)에 "특정정보가 특정인에게 유일하게 속한다는 사실을 확인하고, 이를 증명하는 행위[4]"라고 정의하고 있으며, 미국 연방증거법[5]에서는 "프로세스 또는 시스템이 정확한 결과를 산출하는 데 사용된 증거"라고 정의하고 있다.

2.1.3 기술적 관점에서의 인증

국내 기술표준문서에서 인증은 "실체가 서비스 제공자에게 자신의 신원을 증명하기 위해서 크리덴셜을 이용하는 과정[6]", OECD는 "정보 또는 통신 시스템에서 사용자, 장치 또는 다른 개체의 주장 된 신원에 대한 유효성 및 보증을 확립하는 기능[7]", ITU-T는 "실체의 신원에 대한 보증 제공[8]", 美국립표준기술원(NIST)는 디지털 신원 가이드라인에서

Table 1. Authentication Processing Steps

Steps	Contens
Enrollments and Identity Proofing	· Resolution · Validation and Verificaion · Enrollments & Issue Credential
Authenticaion & Lifecyle Mgt.	· Auth. Req. with Credential · Credential Binding Check · Credentail Lifecyle Mgt. · Record-keeping

Table 2. Types of Authenticators

Types	Authenticators & Auth. Methods
Know	What you Know. ex)password, Q&A etc.
Have	What you Have. ex)phone/app./email/SMS, OTP, certificate, credit card etc.
Charactor (Bio.)	What you Are. ex)finger print, iris, face, signature, pattern of pressing keyboard etc.

Table 3. Identity Proofing & Authentication

	Contents
Iden-tity Proof-ing	An applicant who is to receive a service provides identity proofing to the person providing the service by providing an identifier for confirming his identity in order to apply for a service. ※ Afterwards, the service provider enrolls the person who wants to receive the service after the validation & verification of the information and Issuing credentials which is the proof for the person's identity.
Auth entic ation	The process of using a credential to authenticate that a claimant is a legitimate user to the person providing the service.

1) "인증"이라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말한다.(전자서명법§2.6)

Table 4. Identity Proofing vs. Authentication with Act.

	Act.	Sign. Act.[24]	RealNm Act.[13]	Reporting Act.[15]	E-Fin. Act.[17]
ID Proof	when	Issuing Certificate	• Open Account • Fin. Transaction	• Open Account • Anti Money Laundry	Granting Access Media
	Article	Act.§15.①,⑥ Rules.§13-2	Act.§3.①,⑦ Decree.§4의2	Act.§5-2.①,③ Decree.§10-4	Act.§6.② Recul.§34.3
	Subject	Certification Authority		Financial Co.	
	Object	Applicant Cert.	Financial Consumer		Applicant Acc. Media
	Methods	Identification with ID Cards			
	Remarks	Face2Face IDProof	Out Source IDProof	Money Laundry	-

	Act.	Specialized Fin. Biz. Act.[19]		Credit Info. Act.[22]		
Authentication	when	Pay with Card	Open Card Acc.	PIV Privision & Utilizaion	History Check Use & Provide	Request self check
	Article	Act.§19.②,§19-2,§24 Recul.§24-6.①	Act.§14.②,③,④,§14-2.② Decree.§6-7.③,④, Decree.§6-8.① Credit Info. Act. Decree.§30.③	Act.§32.①,② Decree.§28.④,⑤	Act.§35.① Decree.§30.③	Act.§38.① Decree.§33.①
	Subject	Store	Financial Co. Card Salesmen	Credit Info. Provider/User	Credit information company	
	Object	Card Holder	Card Applicant	Owner for Credit information		
	Methods	Signature			-	
		-	Certificate		-	
		Passwords	-	Passwords	-	
		E-Authentication	-	-	-	
		Biometrics	-	-	-	
		-	The methods by which safety and reliability can be secured in consideration of the types, characteristics, and risks of commercial transactions(Decree.§30.③)			
	Remarks	• Signature (Card=Receipt)	• Personal ID Info. +Signature etc. ※Issuer of ID, Issue date	-	-	-

"사용자, 프로세스 또는 장치의 신원확인[9]", 특히 디지털 인증은 "디지털 신원을 요구하는데 사용되는 하나 이상의 인증자의 유효성을 결정하는 프로세스[10]"라고 정의하고 있다.

또한 NIST(SP 800-63-3), ITU(ITU-T X.1254), TTA(TTAK.KO-12.0248)의 가이드에서 인증처리 단계는 공통적으로 Table 1과 같이 2단계로 정리되며, 인증처리 시 사용되는 인증 수단은 Table 2와 같이 4가지 종류로 대별하고 있다.

2.1.4 소 결

이상과 같이 인증의 개념은 "서비스 신청시 신원확인(이하 '신원확인')"과 "서비스 사용시 본인확인('사용자인증')"의 2가지가 혼재되어 사용되고 있으며, 본 고에서는 다음의 Table 3과 같이 정리하여 사용하기로 한다.

2.2 앱카드와 인증

2.2.1 앱카드

앱카드('13.9월 출시)는 스마트폰에 등록해서 사용하는 신용카드다. 신용카드를 먼저 살펴보면, 신용카드란 "이를 제시함으로써 반복하여 신용카드가맹점에서 결제할 수 있는 증표로서 신용카드업자가 발행한 것[11]"이며, 모바일신용카드는 모바일상에서 신용카드를 사용할 수 있도록 구현된 것으로, 휴대폰의 유심칩에 신용카드를 내려 받는 유심방식과 신용카드 회사가 제공하는 특정앱(앱카드앱)에 신용카드를 등

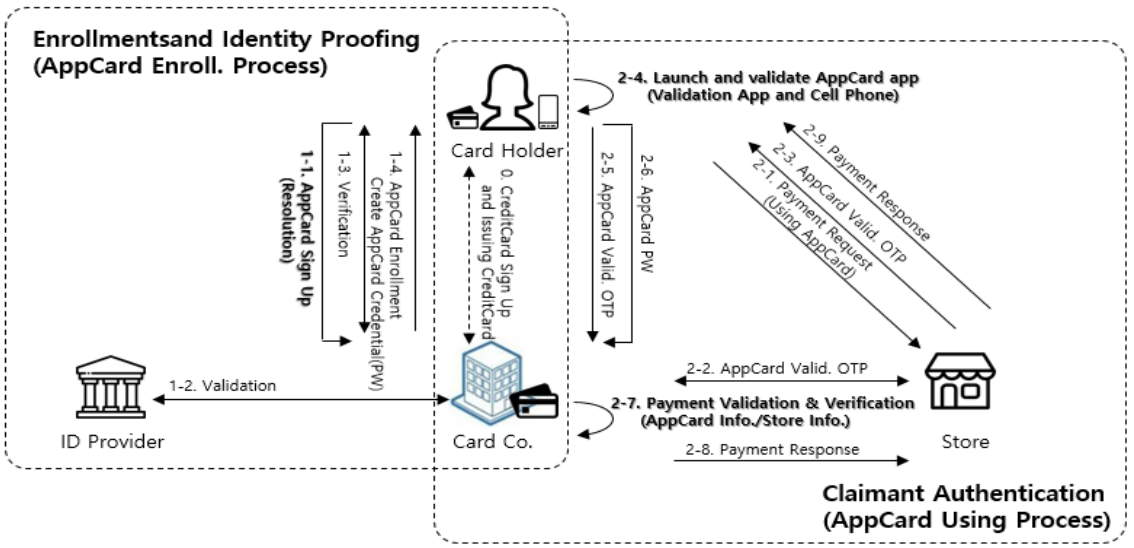

Fig. 1. App Card Service Process

록하여 사용하는 앱방식(이하 '앱카드')로 대별될 수 있다.

앱카드는 전자금융거래법 제2조 제10호 제가목에 따른 전자식카드로 "접근매체"에 해당하며, 앱카드와 신용카드는 전자적 방법에 따른 지급수단으로 사용될 경우 "전자지급수단"에 해당하게 된다.

신용카드 서비스는 "발급", "사용", "정산"의 3단계로 나누어볼 수 있다. "발급"은 카드발급절차[2][12]-카드배송-비밀번호설정 등 "사용"준비가 완료되는 단계, "사용"은 가맹점에서 재화나 용역의 댓가를 결제하는 단계, "정산"은 카드가맹점은 카드사로 부터 카드이용대금을 청구/수령하고, 카드사는 카드이용대금을 회원에게 청구하여 수령하는 단계를 뜻한다. 앱카드는 신용카드 중 한 접근매체에 해당하므로 서비스의 사용단계별 기술/프로세스가 일부 차이가 있을 뿐 개념적으로는 동일하다.

2.2.2 앱카드에서의 인증

법·제도적 관점에서 앱카드와 관련된 인증은 Table 4와 같이 6개법 및 하위규정(금융실명법[13][14], 특정금융정보법[15][16], 전자금융거래법[17][18], 여신전문금융업법[19][20][21], 신용정보법[22][23], 전자서명법[24][25])에 나뉘어 규정되어 있으며, "실지명의의 확인(이하 '실명확인')", "본인확인"으로 대별할 수 있다.

실명확인은 실지명의 여부를 확인하는 것으로 금융실명법 시행령 제4조의2에 따라 주민등록증 등 증표·서류에 의해 확인해야하며, "본인확인"은 행위자가 본인임을 확인하는 것으로 신용정보법 제30조 제3항 후단의 방법[3]에 따라 확인해야한다.

앞서 알아본 인증의 개념과 인증처리관련 가이드를 앱카드와 관련된 인증에 투영해보면 Fig. 1[4]과 같이 신원확인 및 등록 단계와 등록된 사용자의 인증 단계로 나누어볼 수 있다.

신원확인 및 등록단계는 "앱카드 등록"에 해당하는 단계로 앱카드 신청자는 본인의 신원을 증명(identity proofing)을 하고, 추후 본인이 앱카드 사용 요청시 요청자가 본인임을 인증할 수 있는 인증자(authenticator, 휴대폰번호/기기번호 등) 및 서비스 가입을 위한 정보(신용카드 가입자정보 등)를 앱카드 서비스 제공자(신용카드사)에게 전달하며 앱카드 서비스 등록요청을 하고(1-1), 신용카드사는 신청자로 부터 받은 정보를 확인(validation) 및

2) 카드발급절차:본인확인 → 발급불가조건 조회 → 카드발급신청서 및 서류제출 → 결제능력 심사 → 카드발급

3) "신용정보법 시행령 제30조 제3항 후단의 방법은 '금융거래 등 상거래관계의 유형·특성·위험도 등을 고려하여 본인 확인의 안전성과 신뢰성이 확보될 수 있는 수단'을 말한다.

4) NIST, SP 800-63-3[26], IMSAC, Guidance Document: Electronic Authenticaiton[27]을 동조건에 맞게 재구성하였음

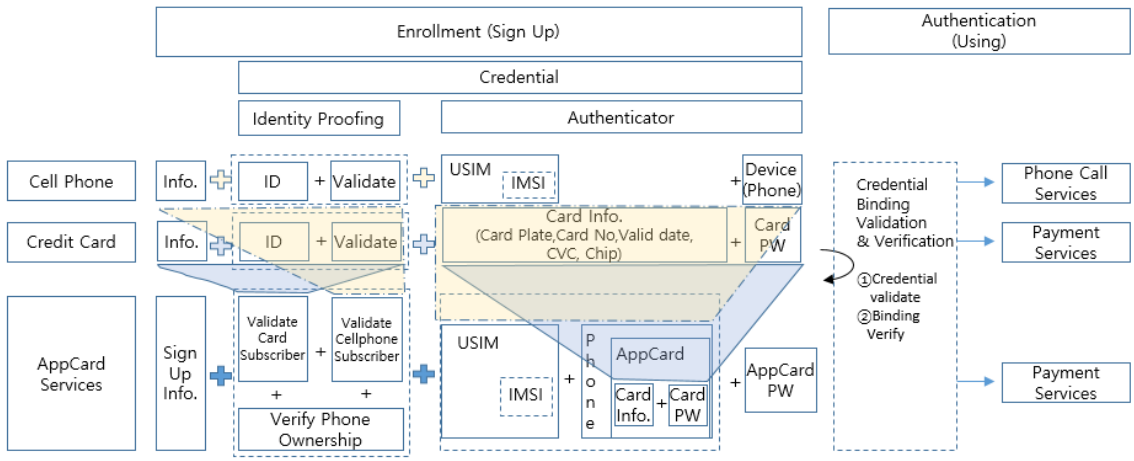

Fig. 2. Enrollment and Authentication Scheme for Cell Phone, Credit Card and AppCard

검증(verification)하고(1-2~3), 앱카드서비스 가입자의 신원과 동 인증자를 연결(binding)하여 자격증명(credential)으로 등록(enrollment)한다(1-4).

사용자 인증단계는 "앱카드 사용"에 해당하는 단계로 앱카드서비스 요청자가 카드가맹점에서 물품을 구매하고 결제요청 시 旣등록된 자격증명(앱카드가 등록된앱을 통해 앱카드 PW입력)을 활용하여, 정당한 사용자임을 신용카드사로 부터 확인받은(2-5) 후 서비스를 제공(결제 승인)한다.

2.3 앱카드 명의 도용사고

앱카드 명의 도용사고('14.9월)는 타인의 신용카드를 자신의 스마트폰에 임의로 등록하여 약 6천여만원의 피해를 일으킨 사건이다.

본 사건은 신원확인 및 등록절차(앱카드등록)에서 신청자와 연결되는 인증자(휴대폰번호) 선정에 문제가 있었으며, 본인확인 절차에서 해당기기 고유의 취약점(안드로이드-스미싱, 아이폰-전화번호 취득불가)이 사용되었고, 이렇게 등록된 자격증명(앱카드PW)은 사용자인증절차(앱카드사용)에서 자격증명으로서의 역할을 할 수 없었던 것이다.

구체적으로 앱카드등록절차에서 사고자는 ①스미싱(Smishing)문자를 통해 피해자가 악성앱을 설치토록하여, 앱카드 등록에 필요한 정보[5]를 유출하고 ② Fig. 1의 앱카드 등록절차에서 자신의 아이폰[6]에 피해자의 전화번호를 도용하여 앱카드 등록신청(1-1)을 한 후 ③앱카드 등록 시 시행되는 본인확인 과정(1-2~3)은 旣탈취한 공인인증서와 旣설치된 악성앱을 통해 SMS인증번호를 탈취하여 통신사 휴대폰명의자 확인을 통과하고, ④사고자가 피해자를 사칭해 앞으로 사용할 앱카드 비밀번호를 설정하였다.

이렇게 등록된 앱카드의 사용절차에서는 앱카드 결제전 앱카드앱의 유효성 및 휴대폰의 정상여부 확인(2-4)을 시행하나, 앱카드 등록신청(1-1) 시 전화번호를 알 수 없었던 것과 동일한 이유로 현재 앱이 사용되고 있는 휴대폰번호를 재확인 할 수 없고, 앞서 사고자가 등록한 앱카드 비밀번호를 결제 시 이용하는 방식으로 범행을 저질렀던 것이다.

이후 각 카드사들은 ARS전화를 이용하여 전화번호(CID)를 취득하는 ARS인증, SMS를 이용하여 CID를 취득하는 앱안심인증 등의 대역외 인증으로 보완하여 운영하고 있으나, 원천문제인 안드로이드의 스미싱취약점과 아이폰의 전화번호 취득불가문제는 해결되지 않고 있는 상태이다.

본 고에서는 동 서비스의 현재상태를 美NIST의 디지털신원 가이드라인에 근거하여 분석해보고 그 대안을 찾아보려한다.

III. 시험 방법

3.1 시험대상 및 방법

본 시험의 대상은 국내에서 스마트폰 앱카드서비스를 실시하고 있는 7개 신용카드사에서 출시한 앱

5) 휴대폰번호, 공인인증서 및 비밀번호 등
6) 아이폰은 앱이 설치되어 있는 휴대폰의 전화번호를 읽을 수 있는 API를 제공하고 있지 않음

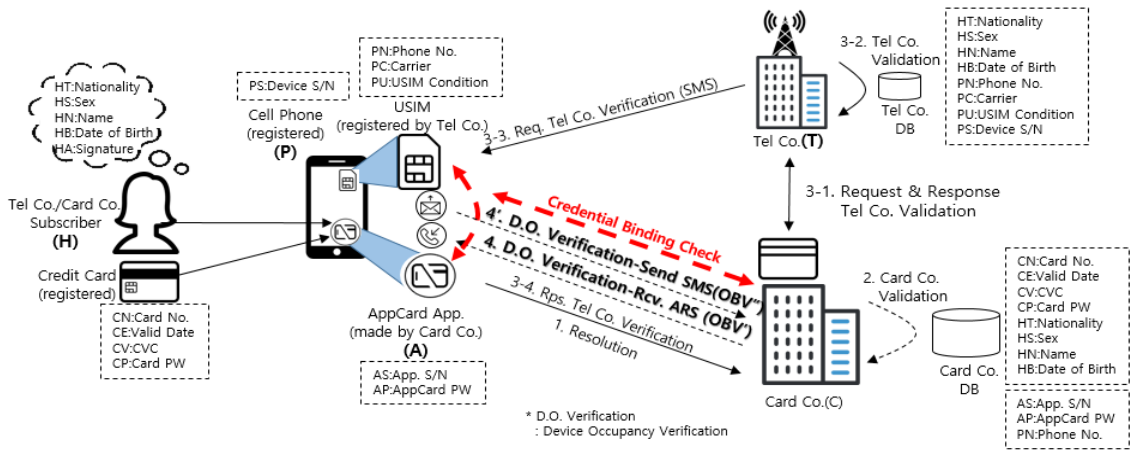

Fig. 3. Identity Proofing for AppCard Enrollment

카드(OS별 각2종)이며, 시험은 2018년 3월에 진행되었다.

본 시험은 시험기간 중에 서비스되고 있던 앱카드 앱의 서비스프로세스를 Table 1과 같이 신원확인 및 등록(앱카드등록절차), 사용자인증 및 등록내용관리(앱카드사용절차)의 2단계로 구분하여, 旣발생한 명의도용사고('14년)의 재현여부를 각 카드사별/스마트폰 운영체제별로 美NIST의 디지털신원 가이드라인(SP 800-63-3)을 요약정리한 Table 3을 적용하여 분석해 보고 그 원인과 해결책을 모색해 보기로 한다.

3.2 인증목적 및 처리단계 분석

3.2.1 신원확인 및 등록단계

신원확인 및 등록단계의 인증(신원확인)목적은 서비스 제공자가 불특정 다수 중에서 자신의 서비스를 신규 신청한 사람을 식별하여 추후 서비스를 제공해야할 대상이 누구인지 확인하는데 있다.

앱카드의 신원확인 및 등록단계의 분석에 앞서 기반이되는 서비스인 휴대전화와 신용카드 서비스에서의 신원확인 및 등록단계를 먼저 분석해보면, 휴대전화는 Fig. 2의 좌측과 같이 신분증 및 신분증 진위확인으로 신원을 확인한 후 확인된 신원과 소지기반 인증자인 휴대폰과 범용사용자식별모듈(USIM) + 휴대전화번호(IMSI)를 결합하여 자격증명으로 지정하고, 신용카드 역시 신분증과 신분증 진위확인으로 확인된 신원과 소지기반(신용카드, 카드번호, CVC, Chip등) / 지식기반(비밀번호) 인증자가 연결되어 자격증명으로 사용된다.

앱카드는 신용카드 가입자에게 발급되는 것으로 ①신용카드가입자의 신원과 휴대폰가입자 신원의 일치여부를 확인하고, ②신용카드정보(소지/지식기반)가 등록된 앱카드앱의 앱일련번호(소지기반)와 그 앱이 설치되는 휴대폰의 전화번호와 기기정보(소지기반)를 결합하고, ③상기②의 앱카드가 발급된 모든 인증자(소지기반)와 상기①의 신원정보(신용카드 및 휴대폰 가입자정보)를 하나로 결합한 후 앱카드 결제용비밀번호(지식기반)를 추가등록하여 자격증명으로 지정하게 된다.

이 중 신원확인단계는 NIST SP800-60A를 적용하면 3단계[28]로 나뉠 수 있는데, 첫째로 대상정보 식별(Resolution)단계는 Fig. 3의 '1.인증정보 수신단계'로 가입신청자의 신상에 관한 지식기반 식별자(HT,HS,HN,HB)과 카드가입자 지위에 관한 소유기반 식별자(CN,CE,CV,CP)와 앱카드앱이 설치된 휴대폰관련 소유기반 식별자(PN,PC,PU,PS)와 앱카드의 사용을 위해 휴대폰에 설치한 앱카드앱 관련 식별자(AS)를 확인할 수 있다. 두번째 단계인 식별정보 확인(Validation)단계는 Fig. 3의 '2.카드사 가입정보 확인' 및 '3.통신사 가입정보 확인'으로 ①카드 가입고객여부 확인을 위해 대상자의 지식기반 신상정보(HT,HS,HN,HB)와 카드사의 인증을 위한 소지기반 식별자(CN,CR,CV)와 지식기반 식별자(CP)를 확인하고, ②앱카드앱을 설치한 휴대폰이 ①의 카드가입고객과 일치하는지 확인을 위해 ①의 신상정보와 앱카드가 설치된 휴대폰 관련 일련

의 정보(PN,PC,PU,PS)를 확인한다. 세번째 단계인 식별정보 검증(Verification)단계는 '4.기기보유여부검증'으로 앱카드앱이 설치된 휴대폰번호(PN)를 재확인하기 위한 단계이다.

3.2.2 사용자인증 및 등록내용 관리단계

사용자인증 및 등록내용 관리단계의 인증(사용자인증)목적은 서비스 제공자가 자신의 서비스에 가입한 고객 중에서 자신의 서비스를 제공하고 그 댓가를 받을 대상이 누구인지 확인하는데 있다.

전 절과 마찬가지 방법으로 휴대전화는 통화요청이 들어오면, 소지기반 인증자인 USIM번호(IMSI 포함)로 서비스 요청자를 식별한 후 정당한 가입자여부를 검증한 후 통화서비스를 제공하고, 신용카드도 결제요청이 들어오면, 카드정보로 서비스 요청자를 식별한 후 사용가능여부를 검증한 후 서비스를 제공한다.

앱카드의 경우는 소지기반 인증자인 앱카드앱의 일련번호(AS)로 가입자를 식별하고, 앱카드(AS),앱카드가 설치된 휴대폰(PN,PC,PU,PS), 카드(CN, CE,CV,CP)간에 여러단계로 묶여있는 자격증명의 유지여부와 지식기반의 앱카드 비밀번호(AP)의 일치여부를 확인한 후 서비스를 제공해야하는 구조로 되어 있다.

3.3 인증처리 단계별 확인 사항

3.3.1 신원확인 및 등록단계

각 카드사별 OS별 앱카드앱에서 실체(신청자)의 신원확인을 위해 사용된 방법과 사용자 등록 시 사용된 인증자를 식별하고, 이 정보가 자격증명으로 사용되기 위해 연결되어 있어야하는 정보(신원+인증자)의 적절성에 대해 확인한다.

3.3.2 사용자인증 및 등록내용 관리단계

같은방법으로 서비스 요청자의 인증을 위해 사용된 인증자를 식별하고, 이 정보가 자격증명으로 사용되기위해 연결되어 있어야하는 정보(신원+인증자)의 적절성에 대해 확인한다.

IV. 시험결과

4.1 신원확인 및 등록단계

4.1.1 대상정보 식별단계

신원확인의 첫번째 단계인 대상정보 식별단계에서 가장 중요한 사항은 식별자를 정확히 취득하는 것이라 할 수 있다. Fig. 2, Fig. 3에서와 같이 이 단계에서는 카드정보(CN등)가 등록되는 앱카드앱(AS)이 어떤 전화번호(PN)를 사용하는 어떤 휴대폰(PS)에서 사용되는지가 엮여서 하나의 식별자로 사용하게 된다. 그 중 카드정보와 앱카드앱 관련정보는 카드사가 생성/통제가능한 부분이나, 휴대폰번호, 휴대폰 기기정보는 휴대폰OS에서 사용할 수 있는 정보(API)에 의존하게된다.

앱카드가 설치되는 휴대폰번호(PN)의 취득을 위해 안드로이드폰에서는 전화번호를 기기(USIM)에서 읽는 반면, iOS폰에서는 전화번호를 휴대폰에서 직접 취득할 수 없어 사용자가 전화번호를 입력(PN′)하게 되어 있었다.

앱카드가 설치되는 휴대폰(PS)과 설치된 앱(AS)을 식별하기 위해서 안드로이드에서는 기기마다 부여된 변하지않는 고유값(UDID)인 휴대폰 기기번호(PS)를 얻은 후 앱이 설치될때 마다 변하는 앱카드앱 일련번호(AS)와 연계하여 기기와 앱을 식별하는 방식을 사용하나, iOS에서는 변하지 않는 고유값 대신 앱에서 기기를 식별하기 위해 생성되는 상대적인 값(UUID)으로 휴대폰 기기번호(PS′)를 취한 후 매 설치 시 마다 변경하는 앱카드앱 일련번호(AS)를 생성하는 경향이 보였다.

4.1.2 대상정보 확인 및 검증단계

신원확인의 두번째/세번째 단계는 취득된 식별자를 확인 및 검증하는 단계로 "확인"단계에서는 전 단계에서 취득한 전화번호의 명의자를 타 기관(통신사)를 통해 확인하여 앱카드서비스를 신청한 사람과 전화번호를 연결하는 의미를 가지고 있다.

확인단계에서 카드사는 통신사를 통해 해당 전화번호의 정당한 가입자가 앱가드서비스를 신청했는지 여부를 확인할 수 있는 반면, 통신사 확인시 입력된 전화번호에 따라 해당 정보의 신뢰성에 큰 차이가 발생할 수 있었다. 전 단계에서 살펴본 바와 같이 전화

Table 5. Identifing Authenticator and Credentials on AppCard

Co.	Step	Android		iOS	
		Phone Number	Dev./App./USIM	Phone Number	Dev./App./USIM
A	Resol.	PN	PS,AS,PU	PN″	AS,PU′
	Valid.	P(PN)=T(PN)	N/A	P(PN″)=T(PN)	N/A
	Verifi.	OBV′(P(PN) =C(PN′)=T(PN)		OBV′(P(PN″) =C(PN′)=T(PN)	
	Cred.	{PN(P,**C,**T)+**PU**+AS+AP}+{CI}+{UI}		{PN(P″,**C,**T)+**PU′**+AS+AP}+{CI}+{UI}	
B	Resol.	PN	Same as A	PN″	Same as A
	Valid.	P(PN)=T(PN)		P(PN″)=T(PN)	
	Verifi.	OBV′(P(PN) =T(PN))		OBV′(P(PN″) =T(PN))	
	Cred.	{PN(P,T)+**PU**+AS+AP}+{CI}+{UI}		{PN(P″,T)+**PU′**+AS+AP}+{CI}+{UI}	
C	Same as B				
D	Same as B				
E	Resol.	PN	Same as A	PN′	AS
	Valid.	P(PN)=T(PN)		P(PN′)=T(PN)	N/A
	Verifi.	N/A		OBV″(H(PN′) =T(PN))	
	Cred.	Same as B		{PN(**P′**,T)+AS+AP}+{CI}+{UI}	
F	Same as E				
G	Resol.	PN′	Same as A	Same as Android	Same as E
	Valid.	H(PN′)=T(PN)			
	Verifi.	OBV″(H(PN′) =T(PN))			
	Cred.	{PN(**P′**,T)+AS+AP}+{CI}+{UI}		Same as Android	

PN : Cell Phone No. (PN′:User input, PN″:SMS CallerID), PU : USIM Check(PU′:2ndary Check with Out of Band)
PS : Cell Phone S/N(PS′ : Alternative Serial by Random Creation)
AP : AppCard Password, AS : AppCard S/N
OBV : Out of Band Verification(OBV′ : Send Encrypted SMS, OBV″ : Receive ARS by PSTN)
CI(Card Info.) : Card No., Valid, CVC, Card PW etc.
UI(User Info.) : Nationality, Sex, Name, Date of Birth etc.

번호를 사용자가 직접 입력(PN′)할 수 있는 iOS의 "확인"단계의 결과에 대한 신뢰성은 매우 낮을 수 밖에 없는 구조를 가지고 있었다.

이러한 문제를 보완하기 위해 각 사별앱에서는 앱과 카드사 서버간 TCP통신을 통한(대역내 통신) 서비스 신청과정에서 고객이 입력한 전화번호(PN′)를 문자 혹은 전화를 이용한 "대역외(Out of Band) 통신"을 통해 "검증"하고 있다.

"암호문자 발신(서비스명 '앱안심인증')"을 사용하는 A~D사는 고객이 입력한 전화번호(PN′)를 암호화하여 문자메시지를 통해 카드사 서버로 송신하여, 카드사에서 문자의 발신번호와 문자내에 암호화된 전화번호를 비교하는 방식으로 해당 전화번호의 정합성을 검증할 수 있는 반면, E~G사는 전화교환망(PSTN)을 통한 자동응답전화(ARS)를 고객이 입력한 전화번호로 발신(서비스명 'ARS인증')하는 방식으로 전화번호를 검증하여 앱이 설치된 휴대폰과 인증전화를 수신한 휴대폰의 동일여부를 확신할 수 없는 문제를 확인할 수 있었다.

4.1.3 소 결

Table 5와 같은 일련의 신원확인단계에서는 추후 사용자 인증단계에서 활용하기 위해 식별/확인/검증의 단계를 통해 식별자(전화번호,휴대폰기기번호,앱카드앱 일련번호 등)를 정확히 취득하여, 신청자-전화번호-휴대폰-앱카드앱과 앱카드비밀번호를 연결하는 것을 목표로 삼고 있으나, OS가 제공하는 API의 차이로 안드로이드가 iOS보다 식별자 취득, 확인 및 검증하기 수월한 환경을 가지고 있었으며, iOS용 앱에서는 이러한 약점을 극복하기 위해 대역외 인증을 사용하였으나, 사용방식 및 특징에 따라 결과의 차이가 있었다.

두 가지 흥미로운 점은 G사의 경우 안드로이드에서도 전화번호를 입력하는 iOS방식으로 구현하여 앱이 설치된 휴대폰의 전화번호(PN)와 고객이 앱내에 전화번호를 입력한 후 ARS인증을 받은 전화번호(PN′)간의 차이가 있을 수 있었으며, C사의 경우 카드사 고객원장에 등록된 전화번호 이외의 휴대폰에

Table 6. Credential Binding Check

<table>
<tr><th rowspan="2">Co.</th><th colspan="3">Android</th><th colspan="4">iOS</th></tr>
<tr><th>non-USIM
(PN_2 ×)</th><th>No.Chg.
($PN_1 \neq PN_2$)</th><th>Other Device
($AS_1 \neq AS_2$)</th><th>non-USIM
(PN_2 ×)</th><th>No.Chg.
($PN_1 \neq PN_2$)</th><th>Telco.Chg.
($PN_1 \neq PN_2$)</th><th>Other Device
($AS_1 \neq AS_2$)</th></tr>
<tr><td>A</td><td rowspan="2">Pass</td><td rowspan="2">Pass</td><td>Fail</td><td rowspan="3" colspan="3">Pass</td><td>Fail</td></tr>
<tr><td>B</td><td>Pass</td><td>Pass</td></tr>
<tr><td>C</td><td rowspan="2">Fail</td><td rowspan="4">Fail</td><td rowspan="4">Fail</td><td rowspan="4">Fail</td></tr>
<tr><td>D</td></tr>
<tr><td>E</td><td>Pass</td><td rowspan="3">Pass</td></tr>
<tr><td>F</td><td>Fail</td></tr>
<tr><td>G</td><td>Pass</td><td>Pass</td></tr>
</table>

앱카드가 설치된 경우 카드사 고객원장에 등록된 전화번호로 관련 알림 메시지(SMS)를 보내주고 있었다.

4.2 사용자인증 및 등록내용 관리단계

앱카드의 “사용자인증 단계”에서 서비스 요청자는 등록자 본인임을 증명하기 위해 전 절에서 신원확인 후 등록된 자격증명을 이용한다. 이를 위해 자격증명으로 연결된 정보(신청자-전화번호-휴대폰-앱카드앱)의 연결에 이상이 없음을 확인한 후 앱카드비밀번호로 증명하는 절차를 활용하게 된다.

이러한 “연결”의 유효성 확인을 위해 ①연결된 전화번호 제거(USIM제거) ②연결된 전화번호를 타 번호로 대체(USIM교체) ③연결된 휴대폰을 타 휴대폰으로 대체(기기교체) 시험을 진행하였으며 그 결과는 Talbe 6과 같다.

앱카드서비스를 제공하기 위해 既등록된 전화번호를 PN_1, 앱카드사용 시 서비스를 요청하는 전화번호를 PN_2라고 할 때, 첫번째 연결된 전화번호 제거는 앱카드 사용요청을 하는 전화번호(PN_2)가 존재하는지 확인하는 것으로 안드로이드는 전화번호(PN_2)의 존재여부 뿐 아니라, 전화번호까지 획득 가능한 반면, iOS는 CTCarrier API[29]를 이용하여 음성통화 가능여부를 확인하는 방식으로 USIM의 존재여부만 확인할 수 있다. 시험결과 실제 USIM이 없는 상황에서 사용이 통제되는 것은 3개사(C·D·F사)의 안드로이드앱에 한했다.

두번째로 전화번호 변경은 既등록된 전화번호를 PN_1과 앱카드사용 시 서비스를 요청하는 전화번호를 PN_2이 동일한지 여부를 확인하는 것으로 안드로이드는 현재 전화번호(PN_2)를 정확히 알 수 있는 반면, iOS는 전화번호을 알 수 없어 대역외 인증으로 대체 통제를 실시한 전절의 예시와 같이 전화번호를 알 수 없으며, 다만 CTCarrier API를 이용하여 통신사만 확인할 수 있을 뿐 전화번호의 변경여부를 확인할 수 없는 근본적인 한계가 있다. 시험결과 5개사(C~G사)의 안드로이드앱에 한해 통제가 되고 있었다.

세번째로 앱카드 설치 후 타 휴대폰에 교체설치를 하고 기존 설치된 휴대폰에서 앱카드가 사용가능한지 여부를 확인하는 것으로 안드로이드, iOS모두 앱설치 시 생성한 앱일련번호(AS_1)와 서비스 요청이 들어온 앱의 일련번호(AS_2)를 비교할 수 있다. 시험결과 1개사(B사)만 복수의 기기에서 동시에 사용하는 것이 가능하였다.

V. 문제점 및 개선방향

5.1 기술적 문제점 및 개선방향

전 장의 시험에서 확인된 바와 같이 일부 OS에서는 자격증명의 요소로 사용되는 전화번호/기기정보의 취득 및 유지여부가 확인 되지 않는 문제가 있었다.

이러한 문제는 ‘14년도 앱카드 도용사고에서 사용된 취약점으로 사고 이후 도입된 대역외 인증이라는 대체수단으로 서비스 가입시 신원확인 단계에서는 취득된 전화번호를 검증하여 도용가능성을 현저히 낮췄으나 등록이후 사용단계에서는 해당 인증자의 유지여부를 확인할 수 없는 문제가 지속확인 되었다. 또한 PSTN(전화교환망)을 이용한 수신방식 ARS인증에서는 다른 휴대폰에서 인증을 받을 수 있다는 문제가 잔존하고 있었다.

이러한 문제는 ①제조사에서 전화번호 또는 식별을 위한 대체 전화번호(암호화 전화번호 등)와 USIM/기기/전화번호 변경확인용 API를 제공해 주

거나, ②통신사에서 과금정보를 활용한 전화번호 확인 서비스를 제공할 경우 해결될 수 있을 것으로 보인다. 최근 Apple에서도 Device Check API[30] 제공 등 기기구분을 추가로 더 할 수 있는 부분이 생겨나고 있다.

5.2 과정(절차)적 문제점 및 개선방향

서비스 신청 및 제공 시 어떤 인증자들이 연결되어 자격증명을 이루고 있는지, 자격증명으로서의 가치를 유지하고 있는지 식별이 되지 못한 문제가 있었고, 이는 해당 내용에 대한 가시성이 부족한 탓으로 보인다.

이를 위해 Table 5, Table 6과 같은 인증자 식별 및 자격증명 유지여부 확인표를 작성하면 문제점을 명확히 짚어낼 수 있을 것으로 보이고, 매 사용 시 마다 이러한 인증자의 정상 연결여부 체크가 필요하다.

또한 OS별로 환경이 다름에 기반한 보완통제(ex. 고액 결제 시 대역외 인증 추가 등)를 고려할 수도 있을 것이다.

5.3 제도적 문제점 및 개선방향

법적으로는 '상거래 관계의 유형·특성·위험도 고려한 안전성과 신뢰성이 확보될 수 있는 수단(신정법령 §30.③)'으로 기술되어 있어 법규 개정 등은 불필요해 보이나, 국내 표준문서에는 인증방법의 보증수준[31], 크리덴셜 관리단계에서 발생가능한 위협 및 보증수준별통제내역[32], 전자거래의 보안위협분류 및 공격기법[33] 등 기술적인 취약점과 등록 시 본인확인문제[34] 위주로만 기술되어, 등록 후 사용단계의 자격증명 유지여부 확인에 대한 절차적인 문제점에 대한 확인 및 통제에 대한 개선이 필요해 보인다.

VI. 결론 및 향후 방향

인증은 모바일 전자금융서비스가 효력을 갖기 위해서 수행되는 중요한 절차다. 인증절차의 잘못된 구현은 과거의 사례와 같은 도용사고로 이어지게 된다. 도용사고 예방을 위해서는 서비스개발 단계에서 부터 해당 서비스가 제공되는 환경에 대한 이해를 바탕으로 명의도용, 인증우회의 가능성을 사전에 분석하여 차단하고, 그렇게 구현된 신뢰관계를 유지하는 것이 필수 불가결한 일이다.

이러한 관점에서 본 논문은 앱카드를 중심으로 스마트폰 전자금융서비스의 인증과정을 NIST의 인증 가이드를 따라 인증자를 식별하고, 확인 및 검증을 하여 자격증명으로 사용되는 일련의 과정을 점검해보는 틀을 제시하였다.

신원확인 및 등록단계에서는 대상자 식별을 위해 취득한 정보와 해당 정보를 확인 및 검증과정을 도식화하여 취약하거나 잘못 선택된 식별자의 선택과 인증과정상의 문제점을 인지하고, 신원확인 이후 서비스 사용을 위한 본인확인 시 사용되는 자격증명을 이루는 요소를 보다 구체적으로 파악할 수 있도록 정리하는 방법을 제시하였다.

그리고 이렇게 파악된 자격증명의 요소는 이후 단계인 사용자 인증단계에서 자격증명이 유효한지 여부를 판단하는 기준으로 활용될 수 있었다.

금번 시험에서 앱카드서비스는 서비스를 제공하는 환경인 스마트폰 OS별로 근본적인 차이가 있어 동일한 방식으로 동등한 서비스를 제공하는 것보다, OS별로 근본적인 환경의 차이를 인식하고 그에 맞는 방식과 수준의 서비스를 제공하는 것이 온당하다고 판단을 하게 되었다.

정부는 최근 공인인증서 제도 폐지를 위해 전자서명법을 개정 중에 있으며, 이에 발맞춰 새로운 인증방법의 등장이 예상된다. 본 연구에서 사용한 방식은 앱카드외 다른 금융서비스뿐 아니라 모든 인증절차에서 인증단계의 평가를 위해 보편적으로 사용할 수 있어, 현업의 실무담당자들이 담당하는 서비스에 신규 등장하는 인증방법을 적용을 위한 평가에 활용될 수 있을 것이다. 다만 각 서비스 고유의 특성과 해당 서비스가 운영되는 고유의 환경은 서비스별로 다른 바 적용 시 이에 대한 고려가 필요할 것이며, 이에 대한 추가적인 연구가 필요하다.

References

[1] Yong-Jae and Young-Mee Shin, "A Historical Examination and Implication of Mobile Payment Servies for the Korean Mobile Transaction Market," The Review of Bussiness History, 31(2), pp. 59, Jun. 2016

[2] TTA, Information and communication

terminology dictionary, http://word.tta.or.kr, Apr. 2018
〔3〕 TTA, Framework for Cerificate Policy and Certification Practice Statement, TTAS.IF-RFC3267, pp. 6, Dec. 2004
〔4〕 §2.6, Digital Signature Act, Act No. 14839, Jul. 2017
〔5〕 US. Rule 901. Requirement for Authentication or Identification (b)(9), Dec. 2011
〔6〕 TTA, Suitable Framework for Entity Authentication Assurance in The Local Environment, TTAK.KO-2.0248, pp. 11, Dec. 2014
〔7〕 OECD, OECD Guidance for Electronic Authenticaion, pp. 7, Jun. 2007
〔8〕 ITU-T, Entity authentication assurance framework, X.1254, pp. 1, Sep. 2012
〔9〕 NIST, Digital Identity Guidelines, SP800-63-3. pp. 47, Jun. 2017
〔10〕 NIST, Digital Identity Guidelines, SP800-63-3. pp. 8, Jun. 2017
〔11〕 §2.3, Specialized Credit Finance Business Act, Act No.15615, Apr. 2018
〔12〕 FSS, "We will inform you of the credit card issuance criteria and issuance procedures," Jul. 2014
〔13〕 Act On Real Name Financial Transactions And Confidentiality, Act No. 14242, May. 2016
〔14〕 Enforcement Decree Of Act On Real Name Financial Transactions And Confidentiality, Presidential Decree No. 28218, Jul. 2017
〔15〕 Act On Reporting And Using Specified Financial Transaction Information, Act No. 14839, Jul 2017
〔16〕 Enforcement Decree Of The Act On Reporting And Use Of Certain Financial Transaction Information, Presidential Decree No. 28687, Feb. 2018
〔17〕 Electronic Financial Transactions Act, Act No. 14828, Apr. 2017
〔18〕 Regulation On Supervision Of Electronic Financial Transactions, FSC Public Notice No. 2016-37, Oct. 2016
〔19〕 Specialiezed Credit Finance Business Act, Act No. 15615 Apr. 2018
〔20〕 Enforcement Decree Of Specialiezed Credit Finance Business Act, Presidential Decree No. 28389, Oct. 2017
〔21〕 Regulation On Supervison Of Specialiezed Credit Finance Business Act, FSC Public Notice No. 2018-2, Jan. 2018
〔22〕 Credit Information Use And Protection Act, Act No. 14823 Apr. 2017
〔23〕 Enforcement Decree Of Credit Information Use And Protection Act, Presidential Decree No. 28387, Oct. 2017
〔24〕 Digital Signature Act, Act No. 14839, Mar. 2017
〔25〕 Enforcement Rules Of Digital Signature Act, Amended By Ordinance Of The Prime Minister No. 996, Oct. 2012
〔26〕 NIST, Digital Identity Guidelines, SP800-63-3, pp. 16, Jun. 2017
〔27〕 IMSAC, Guidance Document: Electronic Authenticaiton, pp. 10, Dec. 2016
〔28〕 NIST, Digital Identity Guidelines Enrollment and Identity Proofing, SP800-63A, pp. 5-6, Jun. 2017
〔29〕 Apple, Swift Developer Documentation "CTCarrier API", https://developer.apple.com/documentation/coretelephony/ctcarrier, Apr. 2018
〔30〕 Apple, Swift Developer Documentation "DeviceCheck API", https://developer.apple.com/documentation/devicecheck, Apr. 2018
〔31〕 TTA, Requirements for E-authenticaion Method of Assurance Level, TTAK.KO-12.0247, pp. 6-11, Dec. 2014
〔32〕 TTA, Suitable Framework for Entity Authentication Assurance in The Local Environment, TTAK.KO-12.0248, pp. 13-25, Dec. 2014
〔33〕 TTA, Authentication Service Guideline for The Layered Risk Level in Online Transaction, TTAK.KO-12.0244, pp. 3-14, Dec. 2014

[34] TTA, Guideline on Identity Proofing Management, TTAK.KO-12.0292, pp. 5-10 Jul. 2016

〈저자소개〉

김 한 우 (Hanwoo Kim) 정회원
2002년 2월: 부산대학교 경제학과 졸업
2010년 2월: 고려대학교 정보보호대학원 석사수료
〈관심분야〉 디지털인증, 보안로그분석, 머신러닝, 정보유출 방지

이 근 영 (Keun Young Lee) 정회원
1992년 2월: 숭실대학교 사학과 졸업
2011년 8월: 고려대학교 정보경영공학전문대학원 석사
2016년 2월: 고려대학교 정보경영공학전문대학원 박사수료
현재: 금융보안원 재직 중
〈관심분야〉 정보법학, 정보보호정책, 머신러닝, 인공지능, IoT보안, 개인정보보호

임 종 인 (Jong In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 및 사이버국방학과 교수, 대검찰청 디지털수사자문위원회 위원장, 국방부 정보화책임관 자문위원, 금융감독원 금융감독자문위원회 자문위원 등
〈관심분야〉 사이버국방, 정보법학, 디지털포렌식, 개인정보보호, 융합기술보안 등

권 헌 영 (Hun Yeong Kwon) 종신회원
1992년 2월: 연세대학교 법학과 졸업
1998년 2월: 연세대학교 법학과 석사
2005년 2월: 연세대학교 법학과 박사
2015년 9월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 정보보호법 및 정책, 정보통신법 및 정책, 사이버법률, 인터넷규제, 전자정부