그래픽 비밀번호를 활용한 공인인증서 개인키 보호방법에 관한 연구

Securing the Private Key in the Digital Certificate Using a Graphic Password

강병훈(Byunghoon Kang)*, 김범수(Beomsoo Kim)**, 김경규(Kyung-Kyu Kim)***

초 록

전자서명법에 근간을 두고 있는 공인인증서는 경제활동 인구의 95%이상이 사용함에 따라 일상생활과 밀접한 관계가 되었고 최근 보안강도 256bit 수준의 암호체계 고도화로 인해 안전성과 신뢰성에 큰 향상이 기대된다. 공개키 기반구조(PKI)를 바탕으로 하는 공인인증서는 보안성에서 큰 문제가 없는 것으로 알려져 왔지만 공인인증서 유출 시 비밀번호 검출 공격에 대한 위협이 존재한다. 기존 연구에서 이러한 취약점을 보완하기 위하여 비밀번호 대체 수단 제공, 공인인증서 저장 매체 확대, 복수 인증방식 등과 같은 다양한 해결방안을 제시하였다. 이러한 방법은 공인인증서의 사용에 대한 보완적 기능을 수행하지만, 비밀번호의 안정성을 보장해주지는 못하는 한계점을 가진다. 따라서 본 연구에서는 비밀번호의 안전성을 높이기 위한 방법으로 비밀번호의 보안강도를 증가시키는 방안을 제시한다. 이에 따라 공인인증서의 관리 보안성과 사용 편리성의 향상이 가능하다. 이 연구는 공인인증서의 보안성 향상과 활용에 관한 기술 개발 및 향후 연구에 활용될 수 있다.

ABSTRACT

A digital certificate mandated by the Electronic Signature Act has become familiar in our daily lives as 95% of the economically active population hold certificates. Due to upgrades to 256 bit level security that have become effective recently, the security and reliability of digital certificates are expected to increase. Digital certificates based on Public Key Infrastructure (PKI) have been known as “no big problem,” but the possibility of password exposure in cases of leaked digital certificates still exists. To minimize this vulnerability, various existing studies have introduced alternative password methods, expansion of certificate storage media, and multiple certification methods. These methods perform enhanced functions but also have limitations including the fact that the secureness of passwords is not guaranteed. This study suggests an alternative method for enhancing the level of password secureness as a way to improve password security. This new method improves security management and enhances the convenience of using

* 연세대학교 정보대학원 석사과정

** 교신저자, 연세대학교 정보대학원 교수

*** 연세대학교 정보대학원 교수

2011년 10월 12일 접수, 2011년 10월 28일 심사완료 후 2011년 11월 17일 게재확정.

digital technologies. The results may be used for developing digital certificate related security technologies and research in the future.

키워드 : 인증, 공인인증서, 비밀번호, 그래픽 비밀번호, 비밀번호 공격, 공개키 기반구조
Authentication, Accredited Certificate, Password, Graphic Password, Password Attack, PKI

1. 서 론

전자서명법[14]은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 1999년 2월 5일 법률 제5792호로 제정되고 2011년 3월 29일 제 8차 (타)일부개정된 법률 제10465호로 개정되었다. 전자서명법[14]은 공개키 알고리즘과 해쉬 알고리즘을 기반으로 하는 전자서명에 법적 인감과 동일한 효력을 부여함으로써, 온라인상의 전자거래를 활성화시키는 제도적 기반을 마련하였고, 전자서명법에 근거하여 2000년 2월 1호 공인인증기관이 지정된 이후 현재 총 5개의 공인인증기관이 지정되어 공인인증서의 발급·관리 업무를 운용하고 있다.

공인인증서는 2011년 2월 기준으로 경제활동 인구의 95% 이상인 2,441만명이 이용하고 있으며, 1999년 제도가 도입된 이후 인터넷뱅킹 및 온라인증권, 보험, 연말정산, 전자세금계산서, 전자조달, 의료, 내자녀 바로 알기 서비스 등 신뢰를 필요로 하는 온라인 전자거래 및 생활전반에서 사용자를 인증하고 전자거래정보의 무결성을 보장하며 전자거래 행위의 부인방지 기능을 제공하고 있다. 공개키 기반 구조(PKI : Public Key Infrastructure) 기반의 공인인증서는 공개키 알고리즘과 해쉬 알고리즘 등 신뢰되고 안전한 거래를 위해 전 세계적으로 사용되는 암호 알고리즘에 의해 발급 및 사용이 보호된다. 또한 행정안전부와 한국인터넷진흥원 주관하에 공인인증서의 안전성 보안강도를 256bit 수준의 암호체계로 고도화를 추진[21]하고 있어 2012년 1월부터는 좀 더 보안성이 강화된 공인인증서가 발급되어 온라인 전자거래의 안전성과 신뢰성을 더욱 향상시킬 것으로 기대된다.

공인인증서에는 공개키가 포함되고 공개키와 쌍을 이루는 개인키는 유출시 보안상의 위험이 있으므로 비밀번호로 암호화되어 보호된다. 현재 한국인터넷진흥원에서 권고하는 안전한 비밀번호는 세 가지 종류 이상의 문자구성으로 8자리 이상의 길이로 구성된 문자열 또는 두 가지 종류 이상의 문자구성으로 10자리 이상의 길이로 구성된 문자열이다[20]. 인간의 기억의 한계 때문에 현재 사용되고 있는 8~10자리 길이의 기억하기 쉬운 비밀번호[30]로 암호화된 개인키는 다양한 해킹공격으로 유출[11, 12]될 수 있고, 유출된 개인키는 비밀번호 검출공격[2, 19]에 의해 복호화되어 불법적으로 사용될 수 있는 취약점을 가지고 있다[29].

본 연구에서는 비밀번호 검출공격으로부터 개인키를 보호하고자, 그래픽 비밀번호를 활용하여 보안강도가 향상된 비밀번호를 유도

하고, 유도된 비밀번호를 활용한 개인키 보호 방법을 제안한다.

2. 문헌 연구

공인인증서는 자연인에게 발급되어 사용되는 것으로 소유자인 본인 외에 타인의 사용을 제한하는 기능이 필요하다. 이를 위해 가장 중요한 개인키를 지식인증기반의 비밀번호로 암호화하여 개인키 비밀번호를 알고 있는 공인인증서의 소유자 본인 외에는 불법적으로 사용할 수 없도록 보호하고 있다. 현재

〈표 1〉 비밀번호 검출 시간〔28〕

비밀번호 조합		영문 대·소문자, 숫자, 특수문자 (96개의 문자열 조합)		
비밀번호		사양		
길이	경우의 수	듀얼코어 PC	워크 스테이션	슈퍼 컴퓨터
2	9,216	Instant	Instant	Instant
3	884,736	Instant	Instant	Instant
4	85 Million	8½초	Instant	Instant
5	8 Billion	13½분	1¼분	8초
6	782 Billion	22시간	2시간	13분
7	75 Trillion	87일	8½일	20시간
8	7.2 Quadrillion	23년	2¼년	83½일
비밀번호 조합		영문 대·소문자, 숫자 (62개의 문자열 조합)		
비밀번호		사양		
길이	경우의 수	듀얼코어	워크 스테이션	슈퍼 컴퓨터
8	218 Trillion	253일	25¼일	60½시간

공인인증서 발급시 개인키 비밀번호 생성정책은 영문 대·소문자, 숫자 그리고 특수문자를 활용한 8자리 이상의 비밀번호이다[20]. 그러나 현실적으로는 많은 사람들이 영소문자와 숫자만으로 구성된 8자리 이상의 비밀번호를 사용한다.

<표 1>은 영국의 웹사이트 'Lockdow'의 'Password Recovery Speeds 보고서[28]의 일부를 인용한 것으로, 영문 대·소문자, 숫자로 구성된 62가지 문자조합과 특수문자를 포함한 96가지 문자조합을 사용하여 비밀번호를 생성 시, 무차별 대입 공격(Brute Force Attack)을 사용하여 비밀번호를 검출해낼 수 있는 대략적인 시간을 보여준다. 96가지 문자조합을 활용한 8자리 비밀번호의 경우 슈퍼컴퓨터에서 83½일/워크스테이션에서 2¼년/듀얼코어PC에서 23년이 소요되고, 현재 공인인증기관에서 공인인증서 발급 시 권고하는 62가지 문자조합의 경우에는 슈퍼컴퓨터에서 60½시간/워크스테이션에서 25¼일/듀얼코어PC에서 253일이 소요된다. 즉, 인간의 기억의 한계 때문에 현재 사용되고 있는 8~10자리 길이의 비밀번호[30]로 암호화된 개인키는 다양한 해킹 공격에 의해 유출[11, 12] 될 경우, 비밀번호 분석을 통해 비밀번호를 유추하고 개인키를 복호화하여 불법적으로 사용할 수 있는 취약점을 가지고 있다[2, 19]. 위와 같은 취약점을 보완하기 위해 가상키보드와 그래픽 비밀번호를 활용한 비밀번호 대체 연구와 공인인증서와 개인키 유출방지를 위한 접근제한 방식의 스마트카드, 저장토큰, 보안토큰, 지문보안토큰 등 저장매체 확대 연구 그리고 보안카드, OTP를 연계한 복수인증 방법 연구를 통해 지식인증기반 비밀번호의 취약점을 보완

해 오고 있다.

하지만 현재까지의 연구는 지식인증기반 비밀번호의 취약점을 가정하고 비밀번호를 대체하거나 접근제한을 위한 저장매체 확대 그리고 복수 인증 방식을 통한 비밀번호 취약점의 보완에 중점을 둔 것으로, 비밀번호 자체의 보안강도를 향상시키기 위한 연구는 거의 진행되지 않았다.

이 연구에서는 비밀번호 자체의 보안강도를 향상시키는 방식을 제안하였고, 현재 지식기반인증에 기반을 두며 복잡한 보안강도를 가지는 그래픽 비밀번호로부터 비밀번호를 유도하고, 유도된 비밀번호를 개인키 암호화 비밀번호로 사용하였다. 유도된 비밀번호는 암호체계 고도화에서 권고하는 보안강도 수준의 안전성을 제공한다. 이로 인해 개인키 비밀번호의 보안강도는 현재 영문 대·소문자와 숫자로 구성된 8자리의 약 50bit 수준의 보안강도에서 약 256bit 수준의 보안강도[21]로 크게 향상되어 웹메일 해킹, 개인PC 해킹, 화면해킹 등을 통해 공인인증서와 개인키가 유출[11, 12]된다 하더라도 공인인증서의 유효기간 내에 개인키 비밀번호를 유추하여 암호화된 개인키를 복호화 할 수 없어 악의적인 목적의 불법 사용으로부터 사용자의 공인인증서를 보호할 수 있다. 또한 그래픽 비밀번호가 갖는 클라이언트-서버모델 특성상 비밀번호 유도를 위하여 서버와 통신을 하게 되는데, 일정수준 이상의 개인키 복호화 시도가 발생하면 사용자에게 알려 공인인증서의 재발급을 유도하거나 또는 한국인터넷진흥원 공인인증서 분실신고서비스와 연동하는 등 공인인증서가 유출되더라도 불법 사용을 위한 비밀번호 검출 공격시도 자체를 무력화시킬 수 있다.

2.1 개인키 비밀번호 취약점 연구

2.1.1 공인인증서

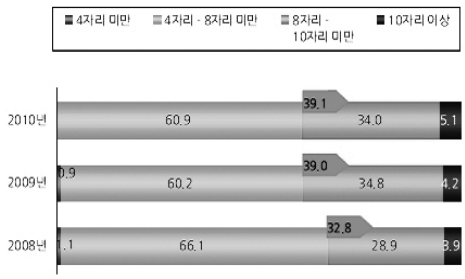
공인인증서는 전자서명법[14]에 따라 엄격한 심사를 거쳐 국가에서 지정한 공인인증기관으로부터 발급되며, 다양한 분야의 전자거래에서 이용되는 인증서이다. 공인인증서로 온라인에서 발생할 수 있는 전자거래의 위·변조를 예방하고 거래 상대방이 누구인지 확인하여 전자거래의 안전을 보장 받을 수 있도록 전자서명을 할 수 있다. 법령에서 서명, 서명날인 또는 기명날인토록 규정한 경우 공인인증서를 이용하여 전자서명을 하면 이와 동일한 효력을 가지게 되어, 법정에서 증거수단으로 사용할 수 있다[14].

2.1.2 개인키 암·복호화

개인키는 소유자 본인만이 사용할 수 있도록 소유자가 설정하는 비밀번호로 암호화되어 보호되고, 복호화되어 사용된다. 개인키 암·복호화는 RSA社의 공개키 암호화 표준#5 (PKCS#5 : Public Key Cryptography Standards#5)에서 정의하고 있는 비밀번호 기반 암호화(PBES1 : Password Based Encryption Scheme)기법을 이용하여 소유자에게서 입력받은 비밀번호를 사용하여 암호화 키와 초기벡터를 생성하고, 생성된 암호화 키와 초기벡터를 사용하여 개인키를 암·복호화한다. 이때 암호화 키와 초기벡터의 생성 및 암·복호화는 한국인터넷진흥원에서 개발한 SEED 블록 암호 알고리즘을 사용한다[22].

2.1.3 개인키 암호화 비밀번호 검출 취약점

지능화되고 다양해진 해킹기술에 의해 공인인증서와 개인키의 유출사고가 발생하고 있다. 공인인증서를 활용하는 대표적인 서비스인 전자금융의 주요 침해사고로 웹메일 또는 개인PC 내에 저장된 공인인증서와 개인키가 유출되어 이체사고 등 금융사고가 발생[12]하였고, 최근에는 화면해킹 기술을 통해 공인인증서와 개인키를 포함한 개인정보를 빼내는 해킹시연이 국정감사 현장에서 시연되었다[11]. 또한 공인인증서 관리 소프트웨어에서 정상적으로 삭제된 공인인증서를 포렌식 툴을 통해 복구하는 것이 가능[7]하다는 연구결과도 발표되었고 이는 해킹위험에 노출되어 있는 공유 컴퓨터에 저장되어 사용된 공인인증서와 개인키가 유출 될 수 있다는 취약점을 드러낸 것이다. 물론 유출된 개인키는 암호화되어 보호된다. 하지만 문제는 하드웨어의 비약적 발전과 개인키 비밀번호 검출 공격 기법[2, 7]에 의해 개인키 비밀번호가 검출될 수 있다는 것이다. <그림 1>에서 보는 바와 같이 사용자는 기억하기 쉬운 8자리 내외의 비밀번호를 사용하는 경향이 있고, <표 1>에서 보는 바와 같이 사용자가 선택한 비밀번호는 임의선택 비밀번호에 비해 분석이 용이하여 비밀번호 검출 위험은 훨씬 증가하게 된다. 또한, 유추한 비밀번호를 입력값으로 독립된 환경에서 무한대로 개인키 암·복호화 시도가 가능하다는 점도 취약점[7]으로 지적되었다.



〈그림 1〉 웹사이트에서 사용 중인 비밀번호 길이[24]

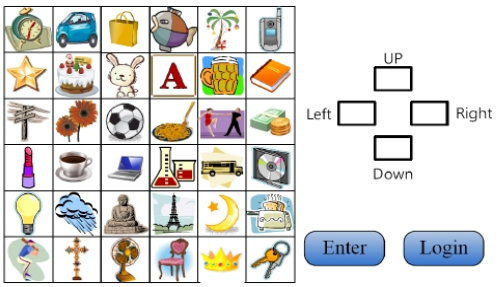
2.2 비밀번호 대체수단 연구

2.2.1 그래픽 비밀번호(Graphic Password)

그래픽 사용자 인터페이스(GUI)로 표현된 사용자 이미지를 사용하는 인증 방식, 이 방식을 사용하는 인증을 그래픽 사용자 인증(GUA : Graphic User Authentication)이라 하며, 그래픽 비밀번호는 문자 비밀번호보다 기억하기 쉽고, 보안성이 높다.

2.2.2 그래픽 일회용 비밀번호(Graphic One-Time Password)

상대적 위치기반의 일회용 비밀번호(ROTP : Relative location based One-Time Password)는 일회용 비밀번호의 동기방식 중 질의응답(Challenge-Response)방식의 하나로 비밀번호인 그림들 간의 상대위치를 이용한 비밀번호 생성방식이다. 그래픽 일회용 비밀번호는 상대적 위치기반 일회용 비밀번호의 대표적인 연구 중 하나이다. <그림 2>에서 별에 대한 노트북의 상대위치는 왼쪽으로 2칸, 위로 2칸 이므로 별을 기준으로 Right에 2칸, Down에 2칸을 입력하면 된다. 즉 상대경로만이 노출될 뿐 대상 그림은 확인할 수 없다[6]. 이 연구에서는 그래픽 일회용 비밀번호 인증과 연동한 개인키 비밀번호 유도 방법을 제안한다.

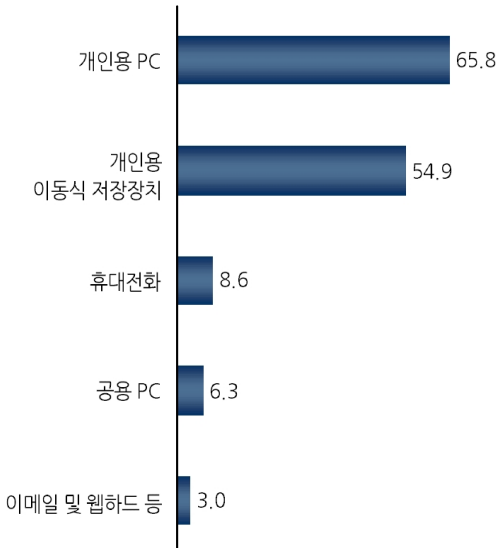


〈그림 2〉 그래픽 일회용 비밀번호

2.3 저장매체 확장을 통한 접근제한 연구

사용자 컴퓨터의 하드디스크[23]에 저장된 공인인증서와 개인키는 상대적으로 해킹공격에 취약하여 외부로 유출될 수 있는 보안위협이 존재한다. 이러한 보안위협에 대응하기 위해 저장매체는 휴대할 수 있고, 연결을 최소할 수 있으며, 저장된 공인인증서와 개인키의 유출이 불가능하도록 접근을 제한하는 방식으로 확대되었다. 초기 메모리타입의 스마트카드인 IC카드 형태와 독자적 파일구조를 지원하는 USB드라이브 방식의 공인인증서와 개인키를 저장할 수 있는 하드웨어 기기인 저장토큰[23]에서 최근에는 전자서명 생성키 등 비밀정보를 안전하게 저장·보관하기 위하여 키 생성·전자서명 생성 등이 기기 내부에서 처리되도록 구현된 하드웨어 기기인 보안토큰[23]과 소유자만이 사용할 수 있도록 지문을 등록하고 공인인증서 사용 시 등록된 지문을 검증하도록 하여 나라장터 등 국가기관 전자조달시스템에서 부정 입찰을 막기 위해 지문정보를 본인 신원확인용으로 사용하는 지문보안토큰[23]까지 확대되었다.

공인인증서를 분리된 저장 공간에 저장하여 물리적 접근을 제한하는 저장매체 확대 개념에서 공인인증서와 개인키를 저장하고 모든 암호화 기능을 저장매체 내에서 가능하게 하는 독립운영 개념으로 확대되었다. 또한 항상 소지하는 편의성 측면의 공인인증서를 휴대폰에 저장하는 단계에서 전자거래 정보를 휴대폰으로 전송하고 휴대폰에서 전자서명을 수행함으로써, 휴대폰 소지 및 소유를 확인하는 인증과 복수의 인증채널을 통한 보안성 향상 측면으로 발전하고 있다. 그러나 <그림 3>에서 보는바와 같이 여전히 과반수 이상의 사용자들은 개인용PC의 하드디스크와 공용PC 그리고 이메일 등 웹하드에 공인인증서를 저장하여 사용하고 있고, 다양한 해킹 사례[12]와 최근 화면해킹 시연[11]를 통해 개인PC와 웹하드 그리고 저장토큰에 저장된 공인인증서와 개인키가 저장매체 연결시점에 외부로 유출될 수 있는 취약점이 확인되었다. 이 연구에서는 공인인증서와 개인키의 유출 이후 보호방법을 제안한다.



〈그림 3〉 공인인증서 저장매체[24]

2.4 복수 인증방식 연구

2.4.1 휴대폰 단문메시지 인증

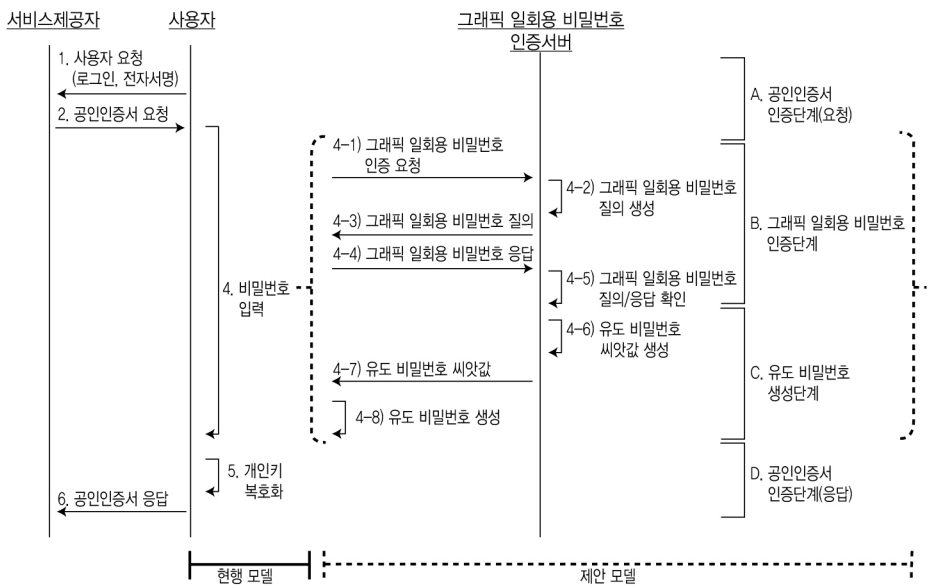
휴대폰이 아닌 다른 접근채널(예 : 유선)을 통해 사용자를 인증할 때 등록된 휴대폰을 소지하고 있는지 인증함으로써, 사용자를 인증하는 서비스이다. 인증이 필요한 경우, 인증서버는 기 등록되어 있는 휴대폰번호로 일회용 인증번호를 단문메시지 형태로 보낸다. 수신자는 단문 문자메시지에 포함된 일회용 인증번호를 접근채널을 통해 인증서버로 보낸다. 인증서버는 일회용 비밀번호를 검증하여 현재 접근채널을 통해 연결된 사용자가 기 등록된 휴대폰을 소지하고 있는 사용자인지를 인증한다. 개인식별번호를 보내 가입한 이동통신사에서 휴대폰 개통 시 등록한 개인식별번호와 검증 후 해당 휴대폰의 소유자인지를 검증하는 소유 검증도 가능하다.

2.4.2 보안카드

보안카드는 소지인증 기반의 인증수단으로 지식인증 기반과 함께 이중요소 인증(2-Factor Authentication) 수단으로 활용된다. 보안대책 강화에 의해 2005년 6월 보안카드 비밀번호를 1개에서 2개의 조합으로 사용하는 방법이 제안되어 현재 사용되고 있다[3].

2.4.3 일회용 비밀번호(OTP : One-Time Password)

1981년 램포트(Lamport)[27]에 의해 처음 제안된 일회용 비밀번호는 인증이 필요한 시점마다 매번 다른 비밀번호를 사용하여 인증하는 방식으로 한번 사용된 비밀번호는 다시 사용되지 않는다. 일회용 비밀번호 단말장치와 인증서버 간에 동기화를 위한 비밀 공유정보인 시간, 씨앗값 등을 공유하고 이 비밀 공유정보를 해쉬함수 등의 암호 알고리즘으



〈그림 4〉 현행 및 제안 모델의 처리 절차

로 일회용 비밀번호를 생성하는 방식이다. 현재 사용하는 비밀번호에서 다음에 사용될 비밀번호 유추가 불가능한 특성과 현재 비밀번호를 재사용할 가능성이 희박한 특성을 가지고 있다[26]. 일회용 비밀번호의 동기화 방식은 네 가지로 나뉘는데, 질의응답(Challenge-Response) 방식, 시간 동기화 방식(Time- Synchronous) 방식, 이벤트 동기화(Event-Synchronous) 방식, 조합(Hybrid) 방식이다[18].

3. 제안 모델

본 장에서는 보안성과 책임추적성을 제공하는 그래픽 비밀번호를 활용한 개인키 비밀번호 유도방법을 제안한다. 제안 모델은 공인인증서 인증단계(요청/응답), 그래픽 일회용 비밀번호 인증단계, 유도 비밀번호 생성단계의 3단계로 구성된다. 공인인증서 인증단계(요청/응답)는 공인인증서를 활용한 필수단계로 현행 모델과의 비교 및 연동을 위한 단계이다. 본 제안은 공개키 기반구조의 공인인증서와 개인키에 대한 제안 모델로 공개키 알고리즘의 특성인 키 분배 기능을 통해 암호화채널을 구성하고 전송되는 데이터는 암호화되어 처리됨을 전제한다. 제안 모델의 전체 처리 절차는 <그림 4>, 제안 모델에서 사용되어지는 주요 시스템 파라미터는 <표 2>에 정리하였다.

3.1 공인인증서 인증단계(요청/응답)

공인인증서 인증은 사용자 인증과 전자거래 인증으로 나뉜다. 사용자 인증은 공인인증서의 유효성을 검증하고 공인인증서 내에 포함되어 있는 공개키와 매칭되는 개인키를 소유하고 있는지 확인하기 위한 과정으로 이루어진다. 요청단계에서 공인인증서와 소유 확인을 위한 임의 데이터의 전자서명 값을 생성하고 임의 데이터와 전자서명 값 그리고 공인인증서를 서버로 제출한다. 응답단계에서 제출된 공인인증서의 경로검증과 폐지여부를 검증하고, 소유확인을 위한 임의 데이터의 전자서명 값을 공개키로 복호화하여 사용자가 올바른 개인키를 소지하였는지를 검증한다. 전자거래 인증은 소유확인을 위한 임의 데이터 대신 전자거래 데이터의 전자서명 값을 생성하고 이를 전자거래 원문 그리고 공인인증서와 함께 서버로 제출한다. 이후 과정은 사용자 인증과 동일하나, 추후 부인방지를 위하여 전자거래 원문과 전자서명 값은 서버에 보관하게 된다. 두 인증단계 모두 전자서명 값의 생성을 위한 개인키가 필요하고, 개인키를 확보하기 위해 비밀번호를 입력받아 암호화된 개인키를 복호화하여야 한다. 이때 입력받는 개인키 비밀번호를 현행모델에서는 키보드 입력 또는 가상키보드를 통해서 입력받게 되고, 제안 모델에서는 그래픽 일회용 비밀번호 인증단계와 유도 비밀번호 생성단계를 거쳐 그래픽 일회용 비밀번호로부터 유도된 개인키 비밀번호를 입력받는다.

3.2 그래픽 일회용 비밀번호 인증단계

그래픽 일회용 비밀번호로부터 비밀번호를 유도하기 위해서는 먼저 그래픽 일회용 비밀번호 인증서버와의 인증을 수행하여야 한다. 이는 해당 개인키의 비밀번호를 생성하는 유도 비밀번호 씨앗 값을 제공하기 이전에 요

청자가 개인키의 소유자임을 확인하기 위한 선행과정이다. 검증을 위한 공인인증서 식별아이디는 인증서에서 추출한 인증서 고유명(DN)과 일련번호(SN)의 조합으로 이루어진다. 인증이력관리를 위해 인증단계는 비밀번호 유도시마다 매번 수행되어야 하고 인증내역은 인증서버에서 관리되어야 한다.

〈표 2〉 시스템 파라미터

기호	의미
U	사용자(User)
AS	그래픽 일회용 비밀번호 인증서버 (Authentication Server)
CID	인증서식별자(Certificate ID)
DN	인증서고유명(Distinguish Name)
SN	인증서일련번호(Serial Number)
IID	아이콘아이디(Icon ID)
IP	아이콘의 행렬 내 좌표(Icon Position)
RP	상대경로(Relative Path)
IR	아이콘간의 관계(Icon Relation)
INO	내가 선택한 아이콘 수(Icon NO.)
II	아이콘별 응답정보(Icon Information)
GQ	그래픽 일회용 비밀번호 질의정보 (Graphic otp Question)
GA	그래픽 일회용 비밀번호 응답정보 (Graphic otp Answer)
GA′	서버 생성 그래픽 일회용 비밀번호 응답정보(Graphic otp Answer)
DPS	유도 비밀번호 씨앗값 (Derived Password Seed)
DPM	유도 비밀번호 중간값 (Derived Password Middlevalue)
DP	유도 비밀번호 (Derived Password)
DNO	유도된 비밀번호 씨앗값의 수 (Derived Password Seed NO.)
Hash	단방향 해쉬함수 * SHA256
||	문자열 연접
PWD	추가로 입력받는 개인키 비밀번호

4-1) 그래픽 일회용 비밀번호 인증 요청

(1) 인증서를 선택한다.

(2) 인증서에서 DN과 SN을 추출한다.

(3) CID를 생성한다.

CID = Hash(DN||SN)

CID U의 공인인증서와 AS간의 식별값으로 활용된다.

(4) CID를 AS로 전송한다.

U -> AS : CID

4-2) 그래픽 일회용 비밀번호 질의정보 생성

(1) CID 등록여부를 판단한다.

수신한 CID와 AS서버의 데이터베이스 내에 저장된 CID 리스트를 비교하여 등록여부를 판단한다. 등록된 CID라면 다음단계를 진행한다. 만약 등록된 CID가 아니라면 그래픽 일회용 비밀번호 서비스 가입절차로 유도한다. 서비스 가입절차는 비밀번호 유도와 무관하여 생략한다.

(2) GQ를 생성한다.

GQ를 구성하는 필수정보는 IID, IP, INO이다.

4-3) 그래픽 일회용 비밀번호 질의

(1) GQ를 U에게 전송한다.

AS -> U : GQ

4-4) 그래픽 일회용 비밀번호 응답

(1) GQ를 활용하여, 자신이 등록한 아이콘을 포함하여 정해진 크기의 행렬 내에 아이콘이 배열된다.

(2) 자신이 선택한 아이콘의 순서에 맞게 각각 IID의 RP를 입력하여 II를 생성하

고 INO만큼 생성된 II를 연접하여 GA를 생성한다(INO ≥ 2).

$II_1 = Hash(IID_1 \| IP_1 \| RP_1)$

$II_1 = Hash(IID_1 \| IP_1 \| RP_1)$

:

$II_{INO} = Hash(IID_{INO} \| IP_{INO} \| RP_{INO})$

$GA = II_1 \| II_2 \| \cdots \| II_{INO} < 1 \cdots INO >$

(3) IID의 IP와 RP 조합이 포함된 GA를 AS로 전송한다.

U -> AS : GA

4-5) 그래픽 일회용 비밀번호 질의/응답 확인

(1) 4-4)과정을 서버에서도 동일하게 수행하여 GA′를 생성한다.

$II_1' = Hash(IID_1 \| IP_1 \| RP_1)$

$II_2' = Hash(IID_2 \| IP_2 \| RP_2)$

:

$II_{INO}' = Hash(IID_{INO} \| IP_{INO} \| RP_{INO})$

$GA' = II_1' \| II_2' \| ... \| II_{INO}' < 1 ... INO >$

(2) 사용자로부터 수신한 GA와 서버에서 생성한 GA′를 비교하여 동일한 경우 다음과정으로 진행한다.

if (GA = GA′) goto 4-6)

else print “오류메시지”

4-6) 유도 비밀번호 씨앗 값(DSP) 생성

(1) 내아이콘 전체의 IID를 연접한 값을 Hash하여 첫 번째 DPS_1를 생성한다.

$DPS_1 = Hash(IID_1 \| IID_2 \| \cdots \| IID_{DNO})$

(2) 내아이콘 전체의 IR를 연접한 값을 Hash하여 값을 연접하여 두 번째 DPS_2를 생성한다.

$DPS_2 = Hash(IR_1 \| IR_2 \| \cdots \| IR_{DNO})$

(3) DSP생성에 IID와 IR이 사용되는 이유는 유일성을 갖는 정보이기 때문이다.

(4) DSP은 정책에 따라 추가로 생성할 수 있다.

DNO = 생성된 DSP의 수

3.3 유도 비밀번호 생성단계

그래픽 일회용 비밀번호 인증이 성공한 경우, 인증서버로부터 유도 비밀번호 씨앗값(DPS)을 제공 받아 유도 비밀번호(DP)를 생성한다. 유도 비밀번호를 생성하는 방식은 제공받은 유도 비밀번호 씨앗값(DPS)를 통합하고 PKCS#5에서 정의하고 있는 PBKDF1 기법[22]을 통해 생성한다. 이때 필요한 솔트값(s)과 반복회수 값(c)은 개인키 내에 포함된 솔트 값과 반복회수 값을 공유해서 사용한다.

4-7) 유도 비밀번호 씨앗값 생성 전달

AS -> S : DPS_1, DPS_2, DNO

4-8) 유도 비밀번호 생성

(1) 정책에 따라 정해진 DNO만큼 DPS를 연접하여 해쉬한다(DNO ≥ 2).

$DPM = Hash(DPS_1 \| DPS_2 \| \cdots \| DPS_{DNO})$

(2) PWD를 추가로 입력받는 경우 PWD와 DP를 연접하여 해쉬한 값이 최종 유도 비밀번호가 된다.

$DPM = Hash(PWD \| DPM)$

(3) DPM과 개인키에서 추출한 솔트값(s), 반복회수(c)을 입력값으로 유도 비밀번호를 생성한다.

$DP = PBKDF1(DPM, s, c, 16)$

4. 제안 모델의 분석

이 연구에서 제안한 모델의 유용성과 효과성을 보안강도, 호환성, 책임추적성 그리고 확장성 측면에서 다음과 같이 분석한다.

4.1 보안 강도

비밀번호 인증시스템의 취약점은 인증 프로토콜이 안전하게 설계되었다 하더라도 비밀번호가 노출된다면 공격자는 노출된 비밀번호를 활용하여 인가된 사용자의 자격으로 인증과정을 통과할 수 있다는 것이다. 공격방법으로 사전 대입공격, 무차별 대입공격이 있으며, 대응방법은 임의 난수형태의 비밀번호를 생성하고, 비밀번호 길이를 증가시키는 것이다[2, 6, 12], [19, 31, 28]. 제안 모델에서 생성된 유도된 비밀번호 씨앗값은 32자 이상의 임의난수형태를 갖는다. 이는 NIST의 전자서명 인증가이드[31]에서 언급된 264.4bit의 보안강도를 갖는 것으로 비밀번호 공격으로부터 안전하다고 할 수 있다. 현재 일반적으로 사용되는 개인키 비밀번호는 8자리의 영문 대・소문자, 숫자 그리고 특수문자를 사용한 96개의 문자조합에서 생성되는 것으로 96^8의 경우의 수로 구성되는데, NIST의 전자서명 인증가이드[31]에서 부분 인용한 <표 3>를 기준으로 약 52.7bit($2^{52.7}$ = 7.316e+12)의 보안강도를 갖는다. 반면 제안된 유도 비밀번호는 난수형태의 16자리로 가정했을 때 약 105.4 bit($2^{105.4}$ = 5.352e+28)의 보안강도로 현재의 비밀번호에 대비해서 약 10e+15배 이상 보안강도가 향상된다. <표 1>을 참고로 동일한 96개의 문자조합에서 7자리에서 8자리로 늘어날 경우, 슈퍼컴퓨터를 기준으로 비밀번호 검출 시간이 20시간에서 83½일로 100배에 가까운 약 83일의 연산시간이 추가로 필요하다는 점을 감안했을 때, 최소 8자리 이상 길이가 늘어난 비밀번호는 공인인증서의 유효기간인 1년 내에는 검출이 불가능하다고 판단된다. 최근 화면해킹[11]을 통해 사용자 컴퓨터의 로컬 시스템과 확장 저장매체 내에 저장된 공인인증서의 유출이 어렵지 않게 가능하다는 것이 소개되었다. 제안 모델의 충분히 높은 보안강도의 유도된 비밀번호로 개인키를 암호화한다면 설사 공인인증서와 개인키가 유출된다고 하더라도 공인인증서 유효기간 내에

〈표 3〉 비밀번호 길이 대비 보안강도〔31〕

(단위 : 비트)

비밀번호 길이	임의선택 비밀번호	
	10개 문자조합	94개 문자조합
1	3.3	6.6
2	6.7	13.2
3	10.0	19.8
4	13.3	26.3
5	16.7	32.9
6	20.0	39.5
7	23.3	46.1
8	**26.6**	**52.7**
10	33.3	65.9
12	40.0	79.0
14	46.6	92.2
16	**53.3**	**105.4**
18	59.9	118.5
20	66.6	131.7
22	73.3	144.7
24	79.9	158.0
30	**99.9**	**197.2**
40	133.2	263.4

암호화된 개인키의 복호화가 불가능하여 그로 인한 피해가 발생하지 않을 것으로 기대된다.

4.2 호환성

유도 비밀번호는 그래픽 일회용 비밀번호 인증 후 해당 인증서버로 수신한 씨앗 값을 통해 생성된 충분한 보안강도를 갖는 비밀번호이다. 이는 비밀번호의 충분한 길이가 확보된 것으로 동일한 비밀번호 규칙체계를 갖는다. PKI기반의 전자서명인증체계의 기술규격인 RSA社의 공개키 암호화 표준#5(PKCS#5 : Public Key Cryptography Standards#5)에서 정의하고 있는 비밀번호 기반 암호화(PBES1 : Password Based Encryption Scheme)기법을 포함하여 비밀번호를 활용하는 모든 기술규격과의 호환성을 제공한다.

4.3 책임추적성

현대사회에서 비밀번호는 지식인증기반의 기본 인증수단으로 많은 분야에서 활용되고 있다. 제안 모델에서는 개인키 비밀번호 유도를 위하여 서버에 접근이 필요하고, 모든 요청내역은 저장되어 관리된다. 즉, 로그인, 전자거래시에 전자서명을 수행 시, 비밀번호 유도를 위하여 인증서버에 접근이 필요하고 이때 모든 내역이 관리되므로 사용자에게 요청이력 조회와 일정 회수 이상의 비밀번호 요청 시도 시 사용자가 정의한 수단으로 사용자에게 알림으로써, 공인인증서가 불법유출 또는 개인키 비밀번호 검출 시도 등 불법시도에 대한 감시 및 대응이 가능하다.

4.4 확장성

제안 모델은 온라인상의 인감증명으로 가장 안전하게 보장되어야 할 공인인증서의 개인키 비밀번호 보안강화를 위한 제안이다. 또한 공인인증서를 선택하고 사용하는 클라이언트 측면의 연동 모델로써 서비스제공자와 독립적으로 연동 및 적용이 가능한 제안이다. 즉 비밀번호를 사용하는 서비스에서 클라이언트 측면의 간단한 연동만으로 비밀번호 자체의 보안성을 한 단계 향상시킬 수 있는 확장성을 가진다. 제안 모델은 공인인증서를 포함한 모든 비밀번호 인증방식 서비스의 보안성 향상을 위한 기술 개발에 활용될 수 있을 것으로 기대된다. 또한 제안 모델은 그래픽 비밀번호 방식 외에 OTP 등 다른 인증방식과의 연동 확장성도 제공한다.

〈표 4〉 기존 모델과 제안 모델 비교

		보안강도 *	책임 추적성	확장성 **
비밀번호 대체	가상키보드	하	불가	상
저장매체 확대	저장토큰	하	불가	중
	보안토큰	하	불가	중
	지문보안토큰	하	불가	하
복수인증	보안카드	하	가능	하
	OTP	하	가능	하
제안모델		상	제공	상

* 보안강도 평가기준(<표 3> 참조).
- 상 : 임의선택 비밀번호 길이 24자리 이상
- 중 : 임의선택 비밀번호 길이 16자리 이상
- 하 : 임의선택 비밀번호 길이 8자리 이상

** 확장성 평가기준
- 상 : 1개 측면 이하 연동개발
- 중 : 2개 측면 이하 연동개발
- 하 : 3개 측면 이상 연동개발

● 확장성 평가 측면 1) 클라이언트 측면 연동개발
2) 서버 측면 연동개발
3) 클라이언트-서버 측면 연동개발
4) 기존 업무 연동개발
5) 사용자 구매부담(별도매체 구매)

4.5 제안 모델과 기존 모델의 비교

공인인증서에서 사용되는 낮은 보안강도의 비밀번호 취약점 관점에서 제안 모델과 기존 연구 모델을 보안강도, 호환성, 가용성, 책임추적성 측면에서 비교하였다.

첫 번째 보안강도는 개인키를 암호화할 때 사용되는 비밀번호 자체의 보안강도에 관한 것으로, 임의선택 비밀번호 방식의 비밀번호 길이를 기준으로 분석하였다. 가상키보드는 입력단계에서의 보호기능을 제공하나 입력받는 비밀번호는 8~10자리 수준의 비밀번호로 낮은 보안강도를 갖는다. 저장토큰, 보안토큰은 입력 방식에서 개인식별번호(PIN)를 한 번 더 확인한다는 차이가 있을 뿐 8~10자리 수준의 개인키 비밀번호로 보안강도는 낮다. 지문보안토큰, 보안카드, 일회용 비밀번호는 각각 바이오 인증, 소지기반인증 등 높은 보안성의 인증과정을 거치지만 이는 비밀번호 자체의 보안강도와 무관하고, 개인키는 암호화되지 않은 상태로 저장되거나 8~10자리 수준의 비밀번호를 사용하므로 보안강도는 낮다. 두 번째 책임추적성은 불법사용 감지 및 조회/알림 기능에 관한 것으로 가능/불가능/제공 측면으로 분석하였다. 클라이언트 서버모델인 보안카드와 일회용 보안토큰이 해당 기능의 제공이 가능하다고 판단되나 현재 해당 기능을 제공하고 있지는 않다. 비밀번호 대체 방식과 저장매체 확대 방식은 클라이언트 연동모델로 해당 기능의 제공이 불가하다. 세 번째 확장성은 관련 기술의 다른 서비스 연동 시 개발업무강도로 클라이언트 측면 연동개발, 서버측면 연동개발, 클라이언트-서버 측면 연동개발, 기존 업무와의 연동개발, 별도 저장매체 활용 등 사용자 구매 부담 등을 고려하여 분석하였다. 가상키보드는 클라이언트 측면의 개발로 서비스 연동이 가능하고 기존 비밀번호 방식의 호환성을 제공한다. 저장토큰, 보안토큰, 지문보안토큰은 클라이언트 측면의 개발로 가능하나 사용자 추가 구매 부담이 필요하다. 지문보안토큰은 현재 특정 서비스에 국한되어 있고, 지문등록 등의 부가 절차의 복잡성이 존재한다. 보안카드와 OTP는 클라이언트 서버측면 개발과 서비스 간 연동 등의 추가 개발 그리고 사용자 구매 부담이 필요하다.

5. 결 론

이 연구에서는 공인인증서의 안전성을 위협하는 개인키 비밀번호 검출 취약점을 보완하기 위한 문헌 연구로 비밀번호 검출 공격, 비밀번호 대체수단, 저장매체 확장, 복수 인증 방법에 대해 분석하였고, 비밀번호 자체의 보안강도를 향상시키는 해결방법으로 그래픽 비밀번호를 활용하여 보안강도가 향상된 비밀번호를 유도하고, 유도된 비밀번호를 통해 개인키를 보호하는 방법을 제안하였다. 제안된 방법으로 개인키 비밀번호는 암호체계 고도화에서 권고하는 256bit 수준의 보안강도를 갖게 되고 다양한 해킹공격으로 공인인증서와 개인키가 유출되어도 개인키 비밀번호 검출에 많은 시간이 소요되므로 공인인증서 유효기간 내에 개인키가 복호화되어 불법 사용되는 2차 피해를 방지할 수 있다. 또한 공인인증서 관련 불법행위를 감지하고 이를 사용자에게 알려 추가 피해를 방지할 수 있는 방법도 제시하였다. 결론적으로 제안 모델은 상

대적으로 높은 보안성, 호환성, 책임추적성, 확장성을 제공하여 공인인증서의 기술개발과 및 비밀번호 인증시스템의 향후 연구에 유용하게 적용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] 강필용, “모바일 혁명시대의 공인인증서 이용 현황 및 정책 방향”, 정보보호학회지, 제21권, 제1호, pp. 51-56, 2011.

[2] 김종회, 안지민, 김민재, 주용식, “GPU에서의 SEED암호 알고리즘 수행을 통한 공인인증서 패스워드 공격 위협과 대응”, 정보보호학회지, 제20권, 제6호, pp. 43-50, 2010.

[3] 김태형, 이준호, 이동훈, “피싱 방지 및 가용성 개선을 위한 PKI기반의 모바일 OTP (One Time Password) 메커니즘에 관한 연구”, 정보보호학회논문지, 제21권, 제1호, pp. 15-26, 2011.

[4] 김현승, 박춘식, “클라우드 컴퓨팅과 개인 인증 서비스”, 정보보호학회지, 제20권, 제2호, pp. 11-19, 2010.

[5] 김현철, 이창수, 이경석, 전문석, “인증서를 이용한 보안성이 강화된 일회용 패스워드 검증 시스템의 설계”, 한국통신학회논문지, 제34권, 제4호, pp. 435-441, 2009.

[6] 박영훈, 서승우, “피싱 방지를 우한 상대적 위치 기반의 일회용 비밀번호 시스템”, 대한전자공학회 2008년 정기총회 및 추계종합학술대회, pp. 297-298, 2008.

[7] 맹영재, 양대헌, 이경희, “모바일 뱅킹에서 비밀퍼즐을 이용한 비밀증명방법과 거래승인방법”, 정보보호학회논문지, 제21권, 제1호, pp. 187-199, 2011.

[8] 송유진, 이동혁, “OTP 기반의 웹서비스 인증 메커니즘 설계 및 구현”, 한국전자거래학회지, 제10권, 제2호, pp. 89-107, 2005.

[9] 안해순, 윤은준, 우종정, 부기동, “난수를 활용한 금융 IC 카드 기반의 상호인증 메커니즘”, 한국정보기술학회논문지, 제9권, 제1호, pp. 127-136, 2011.

[10] 윤은준, 홍유식, 김천식, 유기영, “강력한 패스워드 상호인증 프로토콜”, 전자공학회논문지-CI, 제46권, 제1호(통권 제325호), pp. 11-19, 2009.

[11] 이선아, “국감서 해킹 시연… ‘공인인증서까지 통째로 유출’”, YTN, 2011.

[12] 이정호, “전자금융 침해사고 예방 및 대응 강화 방안”, 정보보호학회지, 제18권, 제5호, pp. 1-20, 2008.

[13] 장은영, 김형종, 박춘식, 김주영, 이재일, “모바일 클라우드 서비스의 보안위협 대응 방안 연구”, 정보보호학회논문지, 제21권, 제1호, pp. 177-186, 2011.

[14] 전자서명법, 법률 제10465호, 2011.

[15] 주승환, 서희석, “멀티터치 환경에서의 다중 입력을 통한 패스워드 기반의 사용자 인증 기법”, 한국시뮬레이션학회논문지, 제20권, 제1호, pp. 39-49, 2011.

[16] 준량, 장인주, 유형선, “비밀키를 이용한 토큰 업데이트 보안 인증 기법”, 한국전자거래학회지, 제12권, 제1호, pp. 89-97, 2007.

[17] 차병래, 고일석, “지문 특징을 이용한 일

회용 암호키 생성기법", 한국전자거래학회지, 제113권, 제1호, pp. 33-43, 2008.

[18] 최동현, 김승주, 원동호, "일회용 패스워드(OTP : One-Time Password) 기술 분석 및 표준화 동향", 정보보호학회지, 제17권, 제3호, pp. 12-17, 2007.

[19] 최윤성, 이영교, 이윤호, 박상준, 양현규, 김승주, 원동호, "삭제된 공인인증서의 복구 및 개인키 암호화 패스워드의 검출", 정보보호학회논문지, 제17권, 제1호, pp. 41-55, 2007.

[20] 한국인터넷진흥원 융합보호 R&D팀, "패스워드 선택 및 이용 안내서", 한국인터넷진흥원, KISA 안내·해설 제2010-22호, 2010.

[21] 한국인터넷진흥원 융합보호R&D팀, "암호 알고리즘 및 키길이 이용 안내서", 한국인터넷진흥원, KISA 안내·해설 제2010- 27호, 2010.

[22] 한국인터넷진흥원 전자인증팀, "암호 알고리즘 규격 v1.21", 한국인터넷진흥원, 2009.

[23] 한국인터넷진흥원 전자인증팀, "공인인증기관 간 상호연동을 위한 사용자 인터페이스 기술규격 v1.82", 한국인터넷진흥원(KISA), 2010.

[24] 한국인터넷진흥원, "2010년 정보보호 실태조사-개인편-", 방송통신위원회, 한국인터넷진흥원, 2011.

[25] 황문영, 고웅, 이동범, 곽진, "모바일 클라우드 컴퓨팅을 이용한 스마트폰 뱅킹에서 공인인증서 관리 방안", 대한전자공학회 2010년 하계종합학술대회, pp. 1873-1876, 2010.

[26] Haller, N., Metz, C., Nessser P., and Straw M., "A One-Time Password System," RFC 2289, IETF 1998.

[27] Lamport, L., "Password authentication with insecure communication," Communications of the ACM, 24, pp. 770-772, 1981.

[28] Lockdown, "Password Recovery Speeds," Lockdown.co.kr, 2009.

[29] L, GONG, MA, LOMAS, RM, NEEDHAM, "PROTECTING POORLY CHOSEN SECRETS FROM GUESSING ATTACKS," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol. 11, pp. 648-656, 1993.

[30] Miller, G. A., "The Magical Number Seven, Plus or Minus Tow : Some Limits on Our Capacity for Processing Information," The Psychological Review, Vol. 63, pp. 81-97, 1956.

[31] NIST, William E. Burr and Donna F. Dodson and W. Timothy Polk, "Eletronic Authentication Guideline," NIST, 2004.

저 자 소 개

강병훈 (E-mail : authism@gmail.com)
1999년~2011년 한국정보인증 팀장
2000년 한국항공대학교 컴퓨터공학과 (학사)
2007년~현재 연세대학교 정보대학원 (석사과정)
관심분야 전자인증, 기기인증, 그래픽인증, 개인정보보호, 암호응용, PKI, GOTP, Privacy

김범수 (E-mail : beomsoo@yonsei.ac.kr)
1999년 미국 University of Texas at Austin, Ph.D.
1999년~2002년 미국 University of Illinois at Chicago, 조교수
2002년~현재 연세대학교 정보대학원 교수
2011년~현재 지식서비스보안과정 및 ITMS과정 주임교수, ISACA Korea 부회장
관심분야 정보보호정책 및 제도, 프라이버시 권리, 전자상거래, 정보경제학

김경규 (E-mail : kyu.kim@yonsei.ac.kr)
1986년 미국 Utah 대학, 경영정보학 (박사)
1986년~2002년 Pennsylvania State University, University of Cincinnati, Nanyang Technological University (Singapore) 등 교수 역임
2001년~현재 연세대학교 정보대학원 교수
관심분야 e-Business Strategy, Trust in B2C e-Commerce, Supply Chain Management, Evaluation of Industrial Informatization, u-biz Strategy