데이터 유출 및 접근방지를 위한 이중 인증방식의 군(軍) 적용방안

정 의 섭*, 김 지 원**, 김 재 현**, 정 찬 기***

요 약

우리나라 인터넷 사용자의 대부분은 공인인증서를 발급받아 이를 이용해 다양한 업무에 사용하고 있다. 이런 이유로 공인인증기관 및 보안관련 업체에서는 공인인증서를 사용자의 데스크톱(PC)에 저장하지 말고 USB메모리 및 휴대용 저장장치에 저장하고 사용하는 것을 권장하고 있다. 이런 노력에도 불구하고 공인인증서의 해킹은 지속적으로 발생하고 금전적 피해도 잇따르고 있다. 또한, 우리 군에서는 보안상의 이유로 일반 사용자에게는 USB를 사용할 수 없게 하고 있다. 그러므로 본 연구는 사용자가 소유한 USB메모리와 PC의 고유정보를 이용한 이중 암호화(Two-factor)방식을 제안하여 일반 사용자에게 안전한 개인키 파일 관리방안을 제시하고자 한다. 나아가 이를 국방에 적용하여 중요자료의 생산 및 보관중인 비밀에 대한 외부유출 및 비인가자의 접근방지에 기여하고자 한다.

Military Application of Two-factor Authentication to Data Leakage and Access Prevention

Jung Ui Seob*, Kim Jee Won**, Kim Jae Hyun**, Jeong Chan ki***

ABSTRACT

Most of the Internet users in Korea are issued certificates and use them for various tasks. For this reason, it is recommended that accredited certification authorities and security related companies and use public certificates on USB memory and portable storage devices rather than on the user's desktop. Despite these efforts, the hacking of the certificate has been continuously occurring and the financial damage has been continuing. Also, for security reasons, our military has disabled USB to general military users. Therefore, this study proposes a two-factor method using the unique information of the USB memory and the PC which is owned by the user, and suggests a method of managing the private key file secure to the general user. Furthermore, it will be applied to national defense to contribute to the prevention of important data and prevention of access by unauthorized persons.

Key words : Military, Two-factor Authentication, Data leakage, Access prevention, authentication

접수일(2018년 11월 30일), 수정일(1차: 2018년 12월 18일), 게재확정일(2018년 12월 30일)

* 아주대학교/NCW학과
** 아주대학교/NCW학과
*** 아주대학교/NCW학과

1. 서 론

온라인 뱅킹 서비스, 주식거래, 온라인 쇼핑 등의 전자거래를 함은 물론 행정업무, 학사업무 등 다양한 분야에 공인인증서를 우리나라 대부분의 인터넷 사용자들은 이용하고 있다. 2017년 한국정보통신진흥원(KISA)의 대국민 전자서명 이용실태 조사에 따르면, 공인인증서는 총 3,388만 건이 발급됐고, 이 중 개인이 받은 건은 3,011만 건으로, 이것은 경제활동 인구를 능가하는 수치이다. 이처럼 공인인증서는 경제활동을 하는 대다수의 사람들이 실생활에 사용 중이며, 온라인상에서 자신의 신분을 증명하는 중요한 수단이 되어가고 있다. 공인인증서의 저장매체 수단 중 가장 높은 비율은 USB 메모리(62.2%)로 나타났고, 다음으로는 PC 하드디스크(56.4%) 등의 순으로 나타났다[1]. 이런 저장매체는 공인인증서의 복사 및 탈취의 가능성이 항상 존재한다는 것을 의미하며 이에 대한위협에 대응하기 위해 기존의 보안토큰이나 USIM 스마트 인증과 같은 서비스가 제공되고 있지만 별도의 금전적 지불이 필요하며, 사용자의 저장매체의 분실 및 개인키 노출에 대한 보호방안도 강구되지 않은 상태이다. 따라서 본 연구에서는 대부분의 공인인증서 사용자들이 공인인증서 저장매체로 사용하고 있는 USB메모리와 개인 데스크톱(PC)을 조합하여 활용하는 Two-Factor 인증방식을 제안하여 공인인증서의 보안을 강화하는 방안을 논하고자 한다.

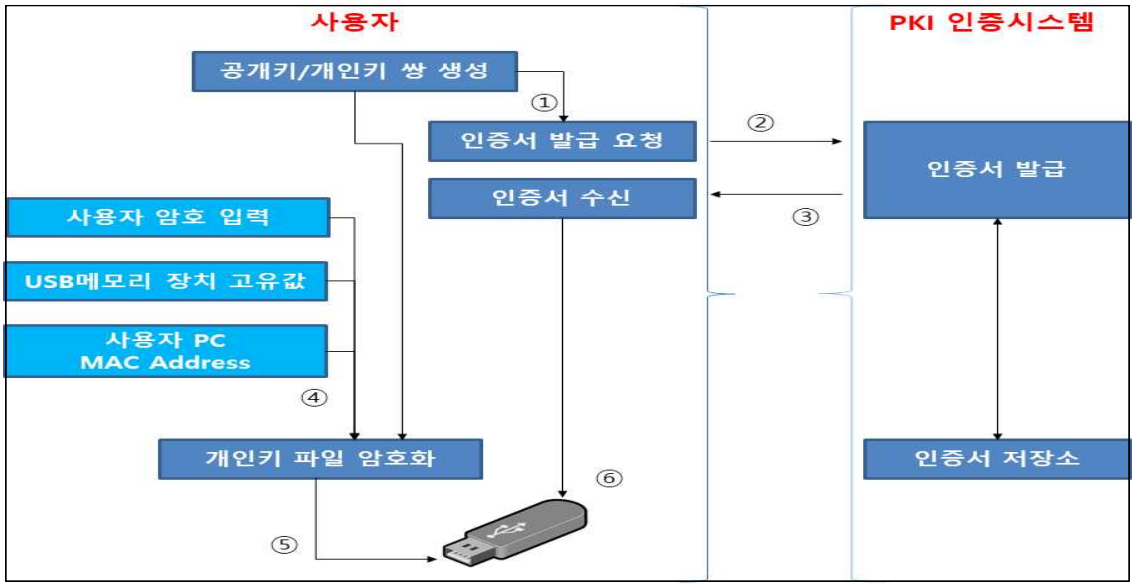
2. 연구배경 및 문제점

공개키 기반구조(Public Key Infrastructure, PKI)는 공개키 암호 방식을 바탕으로 한 디지털 인증서를 활용하는 소프트웨어, 하드웨어, 사용자, 정책 및 제도 등을 총칭하여 일컫는 말이다. 공인인증서는 공개키 증명서, 디지털 증명서, 전자 증명서 등으로 불리며, 개인키와 한 쌍으로 존재한다. 공개키 기반구조(PKI)는 이러한 전자서명을 생성하고 검증하는데 사용되는 개인키와 공개키를 안전하게 나누어주는 역할을 담당하는 신뢰된 제3자(인증기관)의 존재를 전제로 하고 있다[2]. 우리나라의 인증서는 대부분 개인인증서로 사용되며, 인증서의 파일들이 보관 및 저장되는 위치와 방법이 독특하여 웹브라우저로는 사용이 불가능하다. 그러므로 공인인증서를 사용하려면, 이용자가 추가프로그램을 반드시 저장매체에 설치해야만 한다. 이런 문제를 해결하고자 일부 은행에서 '브라우저 인증'서비스를 적용하여 공인인증서를 웹브라우저에 저장해 사용할 수 있도록 하였고, OTP 등을 사용할 시에는 각종 보안 프로그램의 설치 없이도 이것을 이용 가능하게 서비스를 제공할 예정이었으나 아직은 서비스를 오픈할 예정이라고만 하였다[3]. 즉, 현재의 우리나라의 공인인증서는 사용자가 인증서 발급을 요청함에 따라 생성된 공개키 파일, 개인키 파일, 인증서 체인 파일로 구성되어 이러한 파일들을 특정 PC의 하드디스크나 USB메모리에 저장된다는 것을 의미한다. 이렇게 특정 저장매체에 저장된 공인인증서의 정보들은 공격자에게 탈취당해 사용자가 피해를 입을 수 있는 취약점에 늘 노출되어있다. 실제로 한국인터넷진흥원에서 제출한 자료를 보면 2012년 8건에 불과했던 공인인증서 유출 건수는 2013년 8,710건으로 전년 대비 천 배 이상 증가했으며, 2014년에는 4만 1,733건으로 폭증했고, 2016년에는 6,850건이 유출됐다. 공인인증서의 유출이 지속적으로 발생하고 있음을 확인할 수 있는 자료이다[4].

<표 1> 공인인증서 유출현황[4]

연도	12년	13년	14년	15년	16년	합 계
건수	8	8,710	41,733	22,796	6,850	80,097

<표 1>과 같은 공인인증서의 유출을 막기 위해서 악성코드 및 스미싱(Smishing)의 유포지를 탐지해 사전 차단하거나 백신 및 방화벽 설치 및 업데이트 등의 예방방법을 사용하거나 생체인식을 병행한 이중 인증(Two-factor)방식, 또는 사용자의 속성 값을 암호인자로 사용하기도 한다.[8]



(그림 1) 보안된 사용자 인증서, 개인키 등록 절차

업데이트 등의 예방방법을 사용하거나 생체인식을 병행한 이중 인증(Two-factor)방식, 또는 사용자의 속성 값을 암호인자로 사용하기도 한다.[8] 이중 인증방식이란 인증 프로세스에 별도의 보호계층을 추가하는 방법으로 사용자는 비밀번호 이외에 정보를 식별하는 두 번째 부분을 제공하는 방식의 인증방법을 말한다. 현재는 편리성을 강조하여 생체정보인 지문이나 홍채를 이용하는 방법이[5] 대중화 되어 있는데 이러한 생체인식 정보는 생체인식의 정보 자체가 탈취당하면 재발급을 할 수가 없다는 치명적인 단점이 존재한다. 실례로 2015년 미국연방 인사관리국이 해킹을 당해 560만건의 생체정보 유출된 사례와 지위위조기술의 등장 등을 살펴보면 생체인식을 통한 인증의 안전성을 제고해보아야 하는 상황이다.[9]

또한, 공인인증서의 안전한 관리 및 보관을 위해 PC의 CPU칩에 공인인증서를 보관하는 방법인 IPT(Identity Protection Technology)와 TrueCrypt 등이 있으며, 이를 이용하면 암호화시킨 볼륨에 공인인증서를 넣어두어 컴퓨터 해킹이나 USB 메모리 분실 등의 이유로 타인에게 유출되는 것을 방지할 수가 있는데 현재는 개발이 중단된 상태이다.

3. 암호화 시 이중 인증방식

3.1 일반 사용자

일반 사용자가 사용할 수 있는 안전한 공인인증서 보관 방식은 공인인증서 파일이 존재하는 사용자 PC의 MAC 주소 값과 USB 메모리의 고유한 Container ID를 통해 지정된 USB, 지정된 PC에 안전하게 보관하는 이중 인증(Two-factor) 공인인증서 보관방법을 제안하고자 하며 그에 따른 절차는 (그림 1)과 같다.

먼저, 사용자 PC에서 공개키와 개인키 한 쌍을 생성한다. 그 후, 생성된 공개키와 사용자 정보를 인증서 요청 양식에 따라 작성하여 PKI 인증시스템에 사용자의 인증서 발급을 요청하고, 사용자는 인증시스템으로부터 발급된 인증서를 수신한다. 그 후, 개인키 암호용 패스워드와 USB 메모리의 Container ID 값, PC의 MAC 주소 값을 조합하여 해시 값(User_Key)을 생성한다. 해시 값은 아래와 같은 식으로 표현된다.

$$User\_Key = H(UserPW \,||\, 컨테이너\ ID \,||\, MAC\ Address)$$

위와 같은 식으로 생성된 해시 값과 인증서에서 수신한 개인키를 이용하여 암호화 한 후 USB 메모리에 저장하여 활용하는 방식이다.

이 방식은 기존 연구[6]에서 개인키를 생성할 때 단순히 사용자의 패스워드와 USB 장치의 고유한 값으로만 암호화하는 방식이 아니라 사용자가 소유하고 있는 USB와 사용자가 이용하고 사용자만 접근할 수 있는 PC의 고유의 MAC 주소 값을 이용한 다음 다시 해시 값으로 저장하는 인증방식을 제안한다. 이 방식은 해킹으로 인해 개인키 유출 등이 발생해도 해시함수의 특성으로 인해 개인키의 복호화가 불가능하다. 또한, 두 가지의 다른 저장매체의 고유한 값을 요구하기 때문에 USB를 분실하거나 PC의 하드디스크가 해킹 당하더라도 개인키의 안정성을 보장받을 수 있게 된다. 그러므로 실제 인증서를 사용하는 사용자는 등록된 USB와 한정된 PC에서만이 정상적으로 개인키를 복호화 할 수 있게 된다.

또한, 제안한 방식의 객관적인 안전성 평가를 위해 기존에 안전하다고 평가받거나 널리 활용되고 있는 USB 저장방식, USIM 스마트 인증방식, OTP 키 관리방안 방식을 연구에서 제안하는 시스템과 비교하여 평가한 결과는 <표 2>와 같다. 제안한 방식의 장점은 편리성을 생각하여 USB에 저장하는 방식은 동일하며 추가 이용요금이 발생하지 않는다는 것이다. 또한, 해시 값을 이용하기 때문에 탈취된 데이터를 재사용할 수 없으며, 개인키 노출에 따른 재사용도 방지 할 수 있어 기존의 방식보다 안전한 보안성을 제공할 수 있다.

3.2 군(軍) 사용자

본 연구에서 제안한 이중 인증(Two-Factor) 암호화 방안을 군(軍)에 적용하면 비밀의 취급자가 비밀의 생산 및 보관중인 비밀에 대한 자료 유출방지와 타인의 접근통제도 가능하다. 국방 정보화업무 훈령에 따르면 비밀을 생산 및 취급 할 시 비밀 취급인가자가 자신이 취급할 수 있는 비밀의 수준과 자신의 업무와 관련 있는 비밀만 취급할 수 있다. 즉, 타인의 비밀은 해당등급의 비밀 취급인가자가라고 하더라고 열람하여서는 안 된다는 것을 의미한다[7]. 또한, 이 훈령에는 기술적인 방

<표 2> 저장 방식에 따른 비교 평가

방안 / 구분	기존 방식	USIM 스마트인증	OTP 기반 키 관리	**제 안 방 식**
저장매체	USB	스마트폰의 USIM	USB	**등록된 USB**
이용요금	무료	유료	무료	**무료**
인증요소	PW	PW + USIM 카드 암호	PW + OTP	**PW + USB 컨테이너ID + PC MAC Address**
탈취된 데이터 재사용 방지	X	O	O	**O**
개인키 PW 노출에 따른 재사용 방지	X	X	O	**O**
보안성	중	상	상	**상**

안에 대해서는 문서 DRM(Digital rights management)외에는 별도로 명시되어 있지 않고 있다. 문제는 문서 DRM은 기관별 동일한 암·복호화 키를 사용하므로 동일 DRM을 사용하는 기관이라면 타인이라도 파일에 접근 시 복호화가 가능하므로 비밀자료 접근 보안에 취약한 단점이 존재한다. 그러므로 본 연구에서 제안하는 방식을 사용한다면, 비밀의 생산자가 비밀을 생산 시 생산자 PC의 네트워크를 분리한 상태에서 비밀자료를 생산을 하도록 규정한 우리 군에 적용하기에 매우 적합할 것이다. 왜냐하면 비밀의 생산자가 사용하는 PC의 접근은 PC를 사용하는 본인만이 알고 있는 비밀번호로 관리되고 있기 때문이다.

또한, 우리 국방의 환경은 <표 3>와 같이 CMOS 비밀번호를 비롯하여 윈도우 비밀번호 등을 모두 알아야지만 PC에 접근할 수 있어 사용자

의 PC 고유한 값이 보장된다. 그러므로 동일 기관이라도 타인이 비밀 자료에 접근하는 것을 제한할 수 있다.

<표 3> 국방환경의 비밀번호 설정

PC 사용자 비밀번호	설 명
CMOS 비밀번호	PC초기 전원인가 시 메인보드에서 제공하는 비밀번호 제한
운영체제 비밀번호	운영체제 접근을 위한 사용자 비밀번호
화면보호기 비밀번호	사용자가 자리비울 시 화면 잠김 (비밀번호로 보호)
중요자료 보호용 비밀번호	한글과 같은 문서 작성 후 해당 문서에 열람 및 수정제한을 위한 비밀번호

군 사용자가 이용하는 방식을 적용한 방안은 (그림 2)와 같으며 아래와 같은 절차로 진행된다.

1 비밀생산자의 PC에서 비밀자료(secret file)를 생산 한다

2 등록된 USB메모리를 비밀생산자의 PC에 연결한다. 생성된 비밀자료를 암호화하기 위해 암호화용 비밀번호(UserPW)와 PC에 연결된 USB메모리 장치의 컨테이너ID, 비밀을 작업한 PC의 MAC Address값을 이용하여 해쉬값을 계산하고 암호화키를 생성한다. 해시 함수는 x비트의 입력을 y비트의 고정된 출력으로 바꾸어 주는 함수이다. 현재 암호학적으로 안전하기 위해 출력은 160비트 이상이며 이는 해시 함수의 역상 저항성, 제2역상 저항성, 충동 저항성을 보장하기 위해 설정된 수치이다. [10]

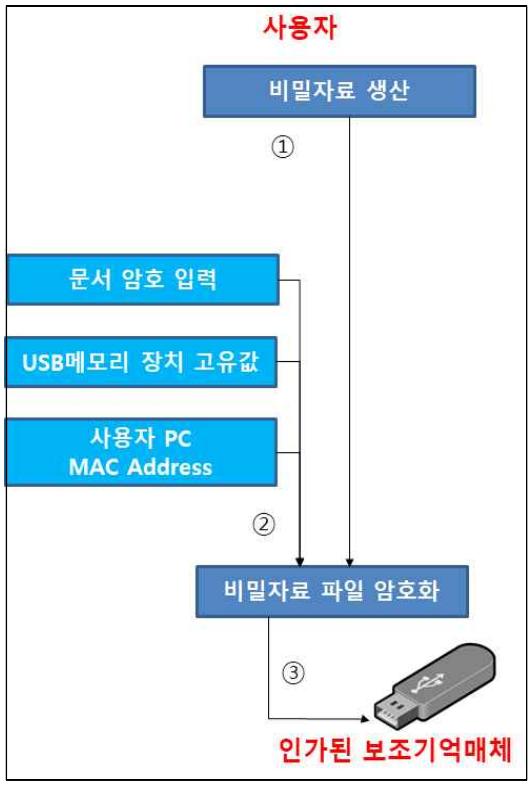
User_Key = H(UserPW // 컨테이너 ID // MAC Address)

- *H : One way collision-resistant hash functions*
- *// : Concatenate operate*

3 생성된 암호화키를 이용하여 비밀자료를 암호화하여 인가된 USB메모리 장치로 저장 후 분리하여 별도의 보관함에 보관한다.

Enc_{User_key} (secret file)

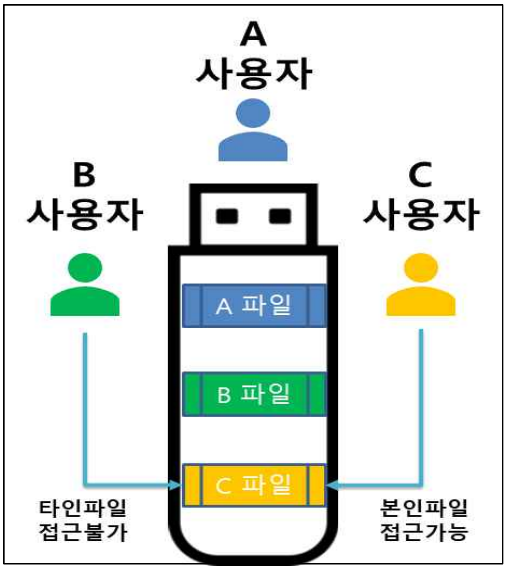
4 복호화의 경우에는 암호화의 과정의 역순으로 이루어지며 복호화 시에 User_Key 생성에 활용되었던 고유한 값 중 하나라도 불일치 할 경우 암호화에 사용된 해시 값의 생성이 불가능하므로 복호화가 불가능하다. 그러므로 타인의 PC에서 복호화 시도 시 복호화가 불가능하게 된다.



(그림 2) 개선된 비밀자료 저장 절차

군 사용자에게 제안하는 이중 인증(Two-factor)방식은 개인별로 보조기억매체를 구분하여 소유하지 않고 대부분 부대 및 부서별로 등록하여 공용으로 사용하며 별도의 비밀보관함에 보관하고

있는 우리군의 상황에 적합하다. 그렇기 때문에 본 연구에서 제안하는 이중 인증(Two-factor)방식을 (그림 2)와 같은 절차를 통한다면 USB 메모리에 저장되는 비밀자료들은 비밀생산자 별로 구분이 되는 PC의 고유 값을 통해 암호화하므로 개개인의 차이가 존재하므로 동일한 USB 저장매체를 사용하는 군 환경이라도 보관된 비밀파일이 본인이 아닌 다른 비밀생산자 및 취급자는 열람이 불가하다. 즉, 비인가자가 타인의 비밀에 접근하기 위해 비밀보관함 등의 통제수단을 뚫고 물리적 방법으로 USB 메모리에 접근할 수는 있겠지만 타인이 생산하고 관리하는 비밀파일은 응용프로그램에서 설정한 비밀번호나 파일암호화용 비밀번호를 알아도 비밀생산자의 PC에 정상적으로 접속하여 열람하지 않는 이상 해당 파일에 접근할 수 없게 되는 것이다. 그림으로 설명하자면 (그림 3)에서 보는 바와 같이, 사용자A는 사용자A의 생산한 파일만 복호화가 가능하고, 사용자B나 사용자C의 파일은 복호화자체가 불가능하게 되는 것이다.



(그림 3) 군 사용자 이용방법

제안한 방식의 평가를 위해 기존 방식과 제안 방식을 비교 평가한 내용은 <표 4>와 같다. 기존에 기관에서 사용자들이 동일한 복호화 방식을 이용하여 타인의 파일도 자유롭게 복호화 가능하였다면 제안방식을 통해 중요파일에 대해 암호화한 파일의 경우 사용자의 인증요소가 만족되어야만 파일이 복호화 되도록 개선되어 보안성을 향상시킨다.

<표 4> 기존 비밀 저장 방식과 비교 평가

구분 \ 방안	기존 방식	**제안 방식**
저장매체	인가된 USB	**인가된 USB**
이용요금(DRM)	기관별 상이	**무료**
인증요소	PW	**PW + USB 컨테이너ID + PC MAC Address**
타인의 파일 접근통제	X (동일 DRM)	**O (고유한 PC와 USB의 값 필요)**
보안성	중	**상**

4. 결론 및 향후연구

공개키 인증방식(PKI)은 지금까지도 훌륭한 알고리즘으로 평가받는다. 그럼에도 불구하고, 악의적인 공격자들에 의해 공인인증서와 비밀번호에 대한 보안사고가 지속적으로 발생하며, 이에 따라 공인인증서의 개인키와 복호화 패스워드의 보관 및 관리의 중요성은 꾸준히 강조되고 있다. 본 연구가 제안하는 USB 메모리와 PC의 고유 값을 활용한 이중 인증(Two-factor)방식은 개인키 파일의 안전한 관리방안을 제안하였다. 또한, 제안방식이 국방 환경에 적합한 중요 군사자료에 대한 데이터 유출방지와 차단하는 방안을 제안하였다.

향후 연구에는 USB 메모리 등 하드웨어 장치 이외에도 다양한 보조기억매체의 암호화에 적

용할 수 있는 센서(Sensor)나 다양한 속성 값들에 대해서도 추가적으로 연구하여 암호화에 활용할 방안을 모색할 필요가 있을 것이라 판단된다.

참고문헌

[1] 한국인터넷진흥원, 17년도 대국민 전자서명 이용 실태조사, 2017.12

[2] B. Kaliski, PKCS #8: Private-Key Information Syntax Standard V1.2, RSA Laboratories, 2008.

[3] 전자신문, 액티브X 없이도 은행·정부서 인증...'브라우저 공동인증' 개발, 검색일 : 2018. 10. 21.

[4] 보안뉴스, 공인인증서 유출현황, 검색일 : 2018.11.1.

[5] 김선종. (2015). 스마트폰 환경에서 공인인증서 사용 시 소유 및 생체인증 연동 방법. 정보보호학회지, 25(6), 13-17.

[6] 김선주, 조인준. (2015). USB 메모리의 컨테이너 ID를 이용한 PKI 기반의 개인키 파일의 안전한 관리 방안. 한국콘텐츠학회논문지, 15(10), 607-615.

[7] 국방부, "국방 정보화업무 훈령", 2018. 02

[8] 한광택,이수연,박창섭. (2014). 국방전산통신망을 위한 국방인증체계(MPKI) 개선 방안에 관한 연구. 융합보안논문지, 14(6), 111-119.

[9] 전정훈. (2016). 바이오 인증 기술의 활성화에 따른 보안 위험성에 관한 연구. 융합보안논문지, 16(5), 57-63.

[10] 김홍태,이문식,강순부. (2014). 군사분야 비밀자료 관리를 위한 암호 알고리즘. 융합보안논문지, 14(6), 141-147.

〔저자소개〕

정 의 섭 (Ui-Seob Jung)
2016년 2월 아주대학교 석사
2017년 3월 ~ 현재
공군 정보체계관리단 정보보호팀 근무
2017년 3월~ 현재
아주대학교 박사과정
email : heaven22@hanmail.net

김 지 원 (Jee-Won Kim)
2002년 2월 동국대학교 학사
2016년 8월 연세대학교 석사
2016년 7월 ~ 현재
육군사관학교 컴퓨터과학과 강사
2017년 3월 ~ 현재
아주대학교 박사과정
email : jeewonkim@ajou.ac.kr

김 재 현 (Jae-Hyun Kim)
1987년~1996년 한양대학교 전산과학사 및 석/박사 졸업
1997년~1998년 미국 UCLA 전기전자과 박사 후 연수
1998년~2003년 Bell Labs, NJ, USA, 연구원
2003년~현재
아주대학교 전자공학부 교수
email : jkim@ajou.ac.kr

정 찬 기 (Chan-Ki Jeong)
1986년 공군사관학교 전자공학 학사
1994년 플로리다공대 전산공학 석사
2001년 플로리다공대 전산공학 박사
2017년 3월 ~ 현재
아주대학교 NCW학과 교수
email : ckjung34@gmail.com