ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 6, pp. 143-148, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.6.143

개인 맞춤형 사용자 인증 시스템 설계

김성열
청주대학교 컴퓨터정보공학과 교수

Design of the Personalized User Authentication Systems

Seong-Ryeol Kim
Professor, Department of Computer & Information Engineering, Cheongju University

요 약 본 논문은 사용자 인증시 사용할 패스워드 키워드를 사용자가 맞춤형으로 정의하여 사용자 인증시 다단계로 사용될 수 있는 개인 맞춤형 사용자 인증 시스템(PUAS)을 설계 제안한다. 제안 개념은 사용자 인증시 서버 시스템 접근시 취득한 패스워드를 다시 사용하는 수동적인 재전송 공격에 강력히 대처할 수 있도록 사용자 인증시 사용될 패스워드 키워드를 사용자가 스스로가 맞춤형으로 정의한다. 인증단계도 단일단계에서 다단계로 확장할 수 있도록 설계한다. 또한 사용자가 정의한 패스워드 관련 정보를 시스템 내에 임의의 암호화된 장소에 저장하도록 설계하여 네트워크의 불법적인 접근을 무력화하도록 설계 제안한다. 따라서 설계 제안한 시스템을 이용하면 침입자가 시스템에 접근하더라도 개인만이 갖고 있는 독특한 개인정보를 통한 패스워드 키워드를 생성하여 개인인증 정보를 생성하고 생성된 인증정보가 저장되어 있는 장소를 알 수 없어 어떠한 수동적 재전송 공격이라도 무력화할 수 있다는 강력한 보안 특성을 갖는다.

주제어 : 재전송 공격, 사용자 인증, 패스워드 키워드, 다단계, 개인 맞춤형

Abstract In this paper, we propose a personalized user authentication system (PUAS) that can be used in multiple stages in user authentication by customizing the password keyword to be used in user authentication. The proposal concept is that the user oneself defines the password keyword to be used in user authentication so as to cope with a passive retransmission attack which reuses the password obtained when the server system is accessed in user authentication. The authentication phase is also designed so that it can be expanded in multiple stages in a single step. Also, it is designed to store user-defined password related information in an arbitrary encrypted place in the system, thereby designing to disable the illegal access of the network. Therefore, even if an intruder accesses the system using the proposed system, it is possible to generate personal authentication information by generating a password keyword through unique personal information possessed only by an individual and not know the place where the generated authentication information is stored, It has a strong security characteristic.

Key Words : Retransmission attack, User authentication, Password keyword, Multiple stages, Personalized

1. 서론

최근에는 인터넷 없이는 일상생활뿐만이 아니라 업무 운영과 수행 등, 각종 사회생활을 할 수 없다 것이 현실이 되었다. 따라서 사용자들이 이용하는 각종 서버들은 기본적으로 UNIX와 윈도우즈 계열 서버 이용이 일반화되었다. 사용자들이 이러한 서버들의 각종 업무들에 접근하기 위하여 접속 시도시에 적법하게 승인된 사용자인가를 확인하는 인증 문제는 향상 중요한 관심사로 대두되고 있다.

*This work was supported by the research grant of Cheongju University(2017.03.01.~2019.02.28.)
*Corresponding author : Seong-Ryeol Kim (srkim@cju.ac.kr)
Received October 4, 2018 Revised November 12, 2018
Accepted December 20, 2018 Published December 31, 2018

적법한 사용자라도 접속과정에서 침입자의 감청으로 ID와 패스워드를 도용하거나 IP 스푸핑(spoofing)이나 스니퍼(sniffer) 등과 같은 해킹기법을 이용하여 ID와 패스워드를 쉽게 도청하여 새로운 침입 수단으로 이용될 수 있다는 문제가 상존한다[1-5].

따라서 본 연구에서는 기존의 사용자 인증 방법인 패스워드 시스템과 패스워드 누출 방지 기술을 고찰하여 각종 네트워크 공격으로부터 강력히 대처할 수 있도록 기존 인증시스템의 일회용 또는 단일단계 패스워드 인증 단계를 다단계로 확장하고 패스워드 키워드를 사용자 맞춤형으로 정의 설정하여 해당 값을 다단계 패스워드로 활용하며 저장된 패스워드 값과 저장 패스워드 파일명을 암호화하여 공격에 의한 패스워드와 패스워드 파일의 접근을 원천적으로 봉쇄할 수 있도록 개인 맞춤형 사용자 인증 시스템(PUAS : Personalized User Authentication System)을 설계 제안한다.

2. 관련연구

관련 연구로는 기본적인 사용자 인증기법과 기본적인 패스워드 노출방지 기법, 강화된 사용자 인증을 위한 패스워드 생성기법들에 관하여 고찰한다[1,3,6,7].

2.1 기본적인 사용자 인증 기법

기본적인 사용자 인증 기법으로는 대부분 ID와 패스워드를 이용하는 인증 방법이 사용되며, 사용자 ID와 대응되는 패스워드 정보를 암호화된 상태로 서버에 저장하고 있다가 접속을 시도하는 사용자의 패스워드를 암호화하여 저장된 값과 일치여부를 확인하여 접속을 허용하는 기법으로 이 경우 장점으로는 구현과 사용이 단순하나, 사용자 패스워드가 단순히 부호화되어 서버로 전달되어 재전송 공격에 대단히 취약하며, 서버는 사용자 ID와 패스워드와 같은 사용자 인증 정보를 관리해야 한다는 부담이 있다[1,2,3,7].

따라서 이러한 문제점을 해결하기 위하여 IP 필터링이라고 하며, 사용자 단말기마다 부여된 IP 주소를 이용하여 서버 접속을 제어하는 네트워크 주소를 이용한 접근제어 기법이 사용되나 시스템 단위로 사용자들의 접근제어를 운용하기 때문에 사용자별 개별적인 접근제어는 기대할 수가 없어 기본 인증 기법과 IP 주소를 이용하여 이를 결합한 형태로 적용하고 있다[1,3].

또 다른 방법으로는 사용자 인증정보를 단일방향성을 갖는 메시지 다이제스트(Message Digest : MD) 함수를 활용하여 서버에 접속시에 필요한 사용자 인증정보를 전송하는 방법인 메시지 다이제스트 인증방법이 이용되기도 한다. 이 방법은 사용자 인증 정보를 MD5와 같은 단일방향 함수를 이용하여 다이제스트하여 전송하면, 시스템는 저장되어 있는 사용자 인증정보와 비교하여 사용자 인증을 수행한다[1,3,7]. 이때 공격자의 재전송 공격을 막기 위해 시간 정보와 함께 전송하며, 이 때 평문 형식의 사용자 인증정보를 메시지 다이제스트하여 결과 값만 저장하고, 평문의 사용자 인증정보는 삭제하여 안전을 보장하도록 한다.

2.2 패스워드 노출방지 기법

사용자 인증시 네트워크상의 도청이나 재전송 공격에 의한 패스워드 노출을 방지하고 재전송 공격에 의한 사용자 패스워드를 보호하기 위하여 S/Key 일회용 패스워드 생성기법이나 Challenge-Response 기법, Time-Synchronous 기법 등과 같은 패스워드 노출방지 기법을 사용한다[1,2,3,7].

S/Key 일회용 패스워드 생성기법은 단방향 함수를 반복적으로 적용하여 일회용 패스워드를 생성하여 사용한다. 즉, 일회용 패스워드는 사용자의 비밀 패스워드를 단방향 함수를 이용하여 특정수만큼 반복적으로 수행하여 생성한다[1,2,7]. 따라서 공격자가 이용된 단방향함수나 특정수의 크기를 알지 못하면 패스워드를 생성할 수 없어 인증시도가 불가능하게 된다.

Challenge-Response 기법은 사용자가 자신의 식별 번호인 PIN(Personal Identification Number) 코드를 인증서버에게 전송하여 난수를 생성하고 challenge로 사용자에게 전달하고 인증서버는 이용자의 패스워드를 찾아 난수의 암호화를 시작하며, 사용자는 Challenge를 전달받아 자신의 패스워드로 암호화하여 인증서버에게 response를 전송하여 이를 이용하여 사용자 인증을 수행한다[1,3].

Time-Synchronous 방식은 인증서버에 저장된 지능형 토큰, 난수생성 알고리즘과 64비트 크기의 비밀키, 사용자의 특정키(PIN)를 이용하여 사용자 인증을 수행한다[1,2,6,8]. 인증시 서버에 저장된 이 모두를 알지 못하면 인증을 할 수 없도록 설계되어 어느 하나만 획득하였다

하더라도 인증에 사용되는 패스워드를 생성할 수 없어 공격자의 인증시도를 무력화할 수 있다.

2.3 다단계 패스워드 생성 기법

기본적인 패스워드를 이용하는 사용자인증 방식은 대부분 초기에 ID와 하나의 패스워드를 한번 등록하여 사용하는 방식인데 이는 등록된 패스워드가 노출될 경우 심각한 보안위협에 노출된다[1,2,3,7]. 따라서 이를 방지하기 위하여 패스워드 등록과 인증단계를 여러 단계로 확장하여 임의의 패스워드를 등록하거나 생성하여 활용하는 방식을 다단계 패스워드 생성기법이라고 한다. 이때 등록 단계를 단순히 소프트웨어적으로 확장할 수도 있고 공인인증서나 PIN 코드, OTP, 생체인식 방법 등을 적용하여 확장하기도 한다. 그러나 등록단계와 적용방식이 복잡하면 보안강도는 높아지나 사용자의 편의성은 다소 떨어질 수도 있어 설계시 확장 단계나 적용방식의 선택은 반드시 사용자의 중요도에 따라 고려해야 한다. 이러한 방식을 적용한 대표적인 솔루션은 RSA SecurID Access, Microsoft Azure AD(Active Directory) 등이 있다[9,10].

RSA SecurID Access[10]는 다중요소 인증 방식을 제공하여 사용자의 정당한 접근방법을 편리하고 안전하게 제공한다. 이러한 RSA SecurID는 하드웨어 및 소프트웨어 토큰을 지원하며, RSA SecurID Access는 사용자가 사용할 수 있는 확장된 인증 방법을 제공한다. 또한 푸시 알림, OTP, 생체 인식(지문 및 아이 프린트 ID) 등을 이용한 인증방법을 제공하고 있어 보안위협에 적절하게 대처할 수 있다.

Microsoft Azure AD[9]는 관리자가 사용자의 추가 인증 방법을 통해 조직과 사용자를 보호할 수 있도록 2단계 인증을 수행하는 Azure MFA(Multi-Factor Authentication)와 셀프 서비스 암호 재설정 기능을 가진 Azure AD SSPR(Self-service Password Reset)으로 구성된다. SSPR과 MFA에서 연결된 기능을 사용할 때 사용자 인증을 위하여 관리자의 보안정책에 따라 인증 방법이나 추가적인 보안 정보를 요구한다. 또한 MFA의 2단계 인증 보안은 계층화된 접근 방식을 기반으로 하여 공격자가 사용자의 패스워드를 알게 된 경우라도 추가적으로 요구하는 인증 보안정보를 알 수 없다면 공격할 수 없어 공격이 무력화할 수 있다.

3. 개인 맞춤형 사용자 인증 시스템(PUAS) 설계

3.1 설계 배경과 개념

일반적인 UNIX계열의 서버들은 사용자인증을 위해 패스워드를 암호화하여 /etc/passwd와 같은 공개된 저장장소에 공개된 파일명으로 저장한다[3,4,6,7]. 또한 패스워드 전송시 평문으로 전송되어 공격자에게 쉽게 노출될 수 있어 보안위협이 상존하게 된다.

따라서 기존의 패스워드 인증 시스템의 문제점을 해결하고자 다음 Table 1과 같은 특성을 갖도록 개인 맞춤형 사용자 인증 시스템을 설계하고자 한다.

Table 1. Characteristic of the proposed system

class.	Present system	Proposed system
password	Send a plain text	Send a cipher text
	Public storage location and filename	Any storage location and filename
Authenticati on phase	Single phase	Multi-phase expansion
	Single fixed keyword	Any user defined keyword

3.2 암호 알고리즘과 보안 에이전트 설계

3.2.1 적용 암호 알고리즘

본 시스템 설계 구현시 적용한 암호 알고리즘은 DCIAS(Device Constant Information user Authentication System)[4] 설계에 적용된 암호 알고리즘을 이용하여 사용자 인증 정보의 암호화・복호화에 사용한다.

3.2.2 보안 에이전트 설계

사용자 인증정보의 암호화・복호화 기능을 수행하기 위한 보안 에이전트는 서버에 존재하며, 사용자 인증에 필요한 사용자 ID와 패스워드의 신규 등록시, 클라이언트로 자동적으로 전송되어 자동 구동을 시작하여 필요한 사용자 인증 정보를 암호화・복호화 작업을 수행하며, 수행 개념도는 다음의 Fig. 1과 같다.

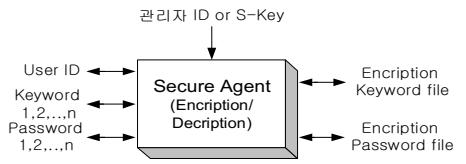

Fig. 1. Diagram of Secure Agent Process

설계한 보안 에이전트는 사용자 클라이언트에 위치하여 사용자 인증정보를 암호화하여 서버에 전송함으로써 네트워크상의 전송 정보는 평문이 아니라 암호화된 정보들이기 때문에 인증정보의 노출을 근본적으로 방지할 수 있다.

3.3 개인 맞춤형 사용자 인증시스템 설계

개인 맞춤형 사용자 인증 시스템 설계개념은 Table 1과 같으며, 기존의 사용자 패스워드 인증 시스템의 인증단계를 한번만 수행하는 단일 단계에서 여러번 수행 가능하도록 다단계로 확장하고, 기존에 암호화된 패스워드가 공개된 /etc/passwd나 /etc/shadow에 저장되어 노출되기 쉬운 패스워드 저장 파일명도 사용자들은 알 수 없도록 암호화된 파일명으로 암호화하여 임의의 저장장소에 저장하여 사용자 인증정보의 노출을 원천적으로 방지할 수 있도록 개인 맞춤형 사용자 인증 시스템을 설계한다. 또한 “패스워드” 또는 “password”라는 단일 키워드도 인증단계 확장에 따라 여러 개의 의미 있는 키워드를 등록하여 사용할 수 있도록 사용자 개인 맞춤형 키워드를 설정할 수 있도록 설계한다.

3.3.1 패스워드 파일 이원화와 파일명 암호화

기존의 공개된 /etc/passwd나 /etc/shadow에 저장되어 노출되기 쉬운 패스워드 파일을 패스워드 값이 저장된 파일과 패스워드 키워드 파일로 분리 설계하여 패스워드 파일의 노출을 방지한다.

또한 패스워드가 저장될 파일의 노출을 막기 위하여 관리자의 ID를 암호키로 사용하여 패스워드가 저장될 2개의 파일명을 암호화하고 ID나 패스워드 파일이 어디에 저장되어 있는지를 알 수 없도록 임의의 디렉토리에 저장함으로써 패스워드 파일의 노출을 원천적으로 막을 수 있도록 설계한다.

3.3.2 인증단계 확장

사용자의 ID와 패스워드를 입력하여 인증 받는 기존의 단일단계 패스워드 시스템에서 설계 제안하는 개인 맞춤형 사용자 인증 시스템에서는 하나의 ID와 패스워드 외에 사용자 개인이 설정한 다른 제2 또는 제3의 패스워드를 입력받아 2중 또는 3중의 인증 단계로 확장하여 다단계화 한다.

다단계 인증의 목적은 단일 인증 단계로부터 오는 침입자의 네트워크상에서 단순한 패킷 분석 방법으로 분석이 가능한 문제를 다단계로 인증함으로 전송 패킷의 연속성을 부여함으로 패킷분석 작업을 어렵게 하고 무력화한다. 패스워드가 암호화되어 암호화된 패킷이 전송됨으로 설상 가로챈다고 하더라도 분석할 수 없게 함으로써 이중 보안 장치를 마련할 수 있다. 그러나 단점으로는 사용자가 하나 이상의 패스워드를 기억해야 하는 문제점은 있을 수 있다.

3.3.3 패스워드의 의미 있는 키워드 등록

인증 단계의 확장에서 오는 사용자가 여러 종류의 패스워드를 기억해야 한다는 단점을 해결하기 위해 패스워드의 의미를 부여할 수 있는 키워드를 사용자가 패스워드를 등록할 때에 함께 패스워드 별명(nick name)을 등록하게 함으로 인증시 사용자가 등록한 패스워드를 쉽게 기억할 수 있도록 설계하여 이 문제를 해결한다.

키워드의 예로서 사번이나 학번, 생년월일, 핸드폰 번호, 군번, 각종 기념일 등등의 사용자만이 잘 알 수 있는 번호나 식별문자를 하나 이상 사용함으로써 패스워드의 노출을 근본적으로 방지하고 또한 패스워드 기억에 관한 노력도 최소화할 수 있다. 만약에 침입자에게 감시되고 있더라도 사용자에 관한 신상 정보를 정확하게 알고 있지 않으면 제2, 제3의 패스워드는 알 수 없어 침입자는 해당 서버에 절대로 침입할 수 없게 된다.

3.4 제안 시스템(PUAS) 모의구현

본 시스템의 구현은 웹에서 구동될 수 있도록 Java와 C++ 언어를 이용하여 모의 구현하였다.

3.4.1 사용자 신규 등록과 정보 수정

사용자 신규 등록시에는 보안 에이전트가 자동적으로 서버로부터 클라이언트로 자동 다운로드 되어 사용자 인증정보를 클라이언트에서 암호화 또는 복호화를 수행하며, 암호화·복호화 기능을 수행하고 종료 후에는 보안 에이젠트는 삭제된다. 사용자인증을 시작하여 나타나는 초기화면은 Fig.2과 같다.

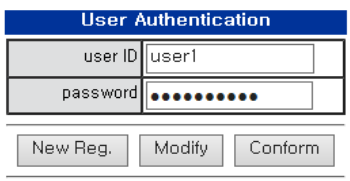

Fig. 2. Initial user authentication

초기화면인 Fig.2에서 사용자의 ID와 사용자 임의의 패스워드 등록하기 위한 키워드인 패스워드 별명과 해당 패스워드 등록은 “New Reg.” 버튼을 클릭하여 Fig. 3과 같은 형식의 화면이 나타나 등록자의 필요한 정보 입력을 요구하도록 설계하였다.

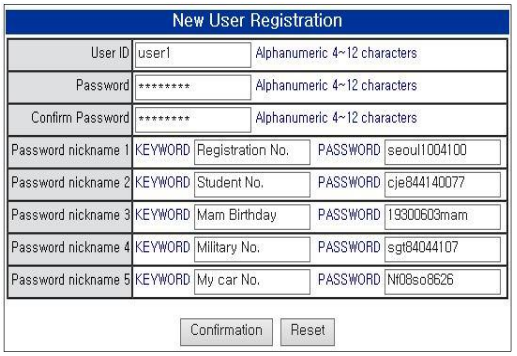

Fig. 3. Registration or modification

사용자 등록시 패스워드 별명인 패스워드 키워드를 사용자가 한개 이상을 등록하면 되지만. 한개만 등록했다면 한번만 사용자 인증을 수행하게 됨으로 본 시스템의 설계 목적을 달성할 수 없으므로 반드시 여러 개의 패스워드 키워드를 등록하는 것이 바람직하다.

3.4.2 관리자 등록과 정보 수정

인증 시스템 관리자는 최초 이 시스템을 설치할 때에 등록하며, 이 관리자 ID를 Key로 사용하여 인증 패스워드 파일인 키워드 파일과 패스워드 파일을 생성하고 관리한다. 관리자는 Fig.2에서 관리자 ID로 로그인하여 “Modify” 버튼을 클릭하면 Fig. 4와 같은 화면에서 요구하는 사용자 정보를 수정하거나 삭제할 수 있다. 또한 일반 사용자는 동일한 방법으로 Fig.3에서 ID를 제외한 사용자의 정보를 수정할 수 있도록 설계하였다.

3.4.3 사용자 인증 수행단계

일반 이용자인 경우에는 사용자 인증 동작만을 수행하며, 신규 사용자일 경우에는 등록후 사용 가능하다.

사용자 인증 수행은 초기 화면인 Fig. 2에서 ID와 패스워드를 입력하여 1단계 인증을 수행하면 Fig.4와 같은 2단계 인증화면이 나타난다.

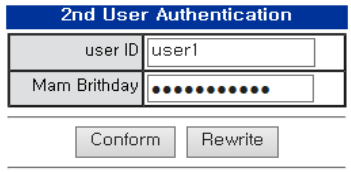

Fig. 4. The 2nd user authentication

해당화면에 패스워드를 입력하고 “Conform”을 누르면 다음 인증단계로 이동하거나 사용자 인증을 종료하고 다음 단계로 이동한다. 따라서 등록된 사용자일 경우 Fig. 4와 같은 인증 단계를 2단계 이상, 다단계로 2차 또는 3차이상의 인증을 수행해야 한다.

3.4.4 생성 패스워드 파일 구성

생성 패스워드 파일은 2개로 하나는 일반 패스워드 값을 갖고 있으며, 또 하나는 패스워드 키워드를 갖고 있는 파일로 저장된 모든 내용과 파일명은 암호화되어 저장되어 있다.

이러한 예로 관리자 ID admin을 Key로 사용하였을 때 생성된 파일 내용은 다음과 같다.

패스워드 파일(13Uq95) 내용 :

xs/NA5rtAk:oCEdTtBJGz2:9atT/1B3E4k:VAW4.zOg
Z0k:54V2Xl9CTaU:0zA5ycASKFI:

키워드 파일(Vm5ZuE) 내용 :

5162:Registration No.:Student No.:Mam
Birthday:Military No.:My car No.:

위의 패스워드 파일명도 13Uq95와 Vm5ZuE로 암호화되어 저장되어 있고, 파일 내용 중에 admin이란 ID를 암호화 결과가 xs/NA5rtAk이며, 키워드 파일의 5162이란 숫자는 admin의 키워드와 패스워드의 매핑 키로 구성되어 있다.

일반 사용자나 공격자는 암호화되어 저장된 2개의 파일이 서버 어디에 존재하는 지 알 수 없다. 또한 해당 파일을 찾아 열어본다 하더라도 암호화되어 있어 구성 내용이 무슨 내용인지를 전혀 알 수 없다. 따라서 본 개인 맞춤형 사용자 인증 시스템은 보다 강력하고 확실한 사용자 인증의 신뢰성과 보안성을 확보할 수 있다.

4. 결론

본 연구는 기존의 패스워드 인증 시스템을 사용자 맞춤 패스워드 키워드 정의형 다단계 패스워드 인증 시스템으로 확장하여 개인 맞춤형 사용자 인증 시스템(PUAS)을 설계 제안하였다.

각종 서버의 사용자 인증 방법으로 기존의 일회용 또는 단일단계 패스워드 인증 단계를 다단계로 확장하고 패스워드 키워드를 사용자 맞춤형으로 정의 설정하여 해당 값을 다단계 패스워드로 활용하며 패스워드 값을 갖고 있는 패스워드 파일 내용과 저장하려는 패스워드 파일명을 암호화하여 기존에 노출 가능성이 상존하는 패스워드 파일의 접근을 원천적으로 봉쇄할 수 있도록 설계하였다.

본 연구 결과, 설계 제안한 인증 시스템은 각종 서버 사용자 인증이나 인터넷을 이용하는 네트워크 사용자 인증 시스템으로 즉시 사용할 수 있다는 장점을 갖고 있다. 또한 침입자의 침입으로부터 도청이나 재전송 공격에 효과적으로 대비할 수 있는 사용자 인증 시스템으로 서버 원시 코드의 변경 없이 기존 시스템에 이식될 수 있다. 따라서 본 연구를 통해 향후 사용자 인증 시스템 연구와 정보보안 분야의 발전에 기여할 수 있을 것으로 기대한다.

REFERENCES

[1] H. G. Kim et al, (2011). A Study on One-Time Password Authentication Scheme in Mobile Environment. *Journal of Korea Multi- media Society, 14(6),* 785-793.

[2] H. R. Ryu et al. (2014). Behavioural Analysis of Password Authentication and Countermeasure to Phishing Attacks - from User Experience and HCI Perspectives. *Journal of Internet Computing and Services(JICS), 15(3),* 79-90.

[3] NCC. (2016. 8). *Information Security.* http://www.nacr.cz/dlm/presentations/dresdner.pdf.

[4] S. R. Kim. (2016). Design of a User Authentication System using the Device Constant Information. *Journal of Convergence for Information Technology, 6(3),* 29-35.

[5] S. Hong. (2014). ARP spoofing attack and its countermeasures. *Journal of Convergence for Information Technology, 4(1),* 47-53.

[6] I. G. Jeun. (2011). *Domestic password usage and encryption Implementation Guide,* KISA.

[7] P. Cobbaut. (2015). *Linux Security.* http://linux-training.be/linuxsec.pdf

[8] S. Shin & K. Han. (2015). A Study Intergrated ID Authentication Protocol for Web User. *Journal of Digital Convergence, 13(7),* 197-205. DOI : 10.14400/JDC.2015.13.7.197

[9] Microsoft. (2018). *Azure Network Security,* Microsoft.

[10] RSA. *RSA SecurID®Access.* https://www.rsa.com/ko-kr/products/rsa-securid-suite/rsa-securid-access.

김 성 열(Seong-Ryeol Kim) [정회원]

- 1982년 숭실대학교 전자계산학과 (공학사)
- 1987년 숭실대학교 대학원 전자계산학과(공학석사)
- 1992년 숭실대학교 대학원 전자계산학과(공학박사)
- 1984년~1990년 오산대학 전자계산과 교수
- 1997년~1998년 호주 QUT ISRC 객원 교수
- 1990년~현재 청주대학교 컴퓨터정보공학과 교수
- 관심분야 : 컴퓨터네트워크, 컴퓨터보안, IT융합기술, 사물인터넷
- E-Mail : srkim@cju.ac.kr