디지털인감을 이용한 일회용 비밀번호 인증 프로토콜의 제안

A Proposal of One-Time Password Authentication Protocol using DigitalSeal

정창훈*, 민대홍*, 양대헌*, 이경희**[1)]
Changhun Jung, Daehong Min, DaeHun Nyang, KyungHee Lee

(22212) 인천광역시 미추홀구 인하로 100 인하대학교 하이테크센터 1008호 정보보호연구실*
(18323) 경기도 화성시 봉담읍 와우안길 17 수원대학교 전기공학과**
jcptk677@gmail.com, mang@isrl.kr, nyang@inha.ac.kr, khlee@suwon.ac.kr

요 약

디지털인감이란 사용자 인증을 위한 데이터가 포함되어 있는 바코드를 스캔하면, 바코드 데이터와 비밀키 그리고 HOTP 알고리즘을 이용하여 HOTP Tag를 LCD에 출력해주는 보안 도구이다. 이 논문에서는, 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜을 제안한다. 사용자는 자신의 아이디, 랜덤챌린지, 디지털인감을 이용하여 로그인을 시도할 때마다 일회용 비밀번호 역할을 하는 HOTP Tag를 생성하여 인증을 할 수 있다. 이를 통해 사용자는 비밀번호를 기억할 필요가 없으며, 여러 웹사이트에 등록된 비밀번호를 일일이 관리하지 않아도 된다는 사용성 측면의 이점을 얻을 수 있다. 또한 MitM, MitB 공격을 방어할 수 있고, 안전하게 비밀키를 사용할 수 있다는 보안성 측면의 이점을 얻을 수 있다.

Abstract

DigitalSeal is a security tool that scans a barcode which includes information for authentication, and then prints HOTP Tag on LCD using the barcode data, a secret key and HOTP algorithm. In this paper, we propose a secure password authentication protocol using DigitalSeal. A user can generate HOTP Tag when trying to login on a website using a ID, a random challenge and DigitalSeal. Then, the user can authenticate on the website using HOTP Tag that serves as an one-time password. As a result, the user can get benefit of usability aspect because it does not have to remember a password and manage a password on multiple websites. In addtion, this protocol is strong against MitM, MitB attacks and a secret key can be more securely managed.

키워드: 디지털인감, 아두이노, 일회용 비밀번호, 인증, 프로토콜
Keyword: DigitalSeal, Arduino, One-Time Password, Authentication, Protocol

1) 교신저자

논문투고일자 : 2018. 07. 18 심사일자 : 2018. 07. 23 게재확정일자 : 2018. 08. 24

1. 서론

정보화시대가 도래하고 네트워크가 발전함에 따라 사용자들은 스마트폰 또는 PC를 이용하여 다양한 온라인 서비스를 이용할 수 있게 되었다. 사용자들은 자신의 계정에 로그인하여 온라인으로 뱅킹, 게임, 메일, 뉴스 등의 다양한 서비스를 이용할 수 있으며 지속적으로 다양한 서비스, 컨텐츠 등이 개발됨에 따라 온라인 서비스 사용자 수는 급격히 증가하고 있는 추세이다. 한국은행에서 보도한 자료[1]에 의하면 2017년 국내은행의 인터넷뱅킹(모바일뱅킹 포함) 등록 고객수는 1억 3,505만 명으로 전년대비 10.2% 증가된 것으로 확인되었다. 한국콘텐츠진흥원에서 보도한 자료[2]에 의하면 2016년 국내 게임시장 규모는 10조 8,945억 원으로, 전년대비 1.6% 증가되었으며 2017년에는 11조원 시장에 진입할 수 있을 것으로 전망하고 있다.

뱅킹, 게임 등의 온라인 서비스 사용자 수가 증가함에 따라 악성 공격자들이 온라인상의 개인 정보를 탈취하여 사용자들에게 금전적인 피해를 주는 사례가 많아지고 있다. 경찰청 통계자료 중 사이버범죄 발생 및 검거 현황[3]에 의하면 2014년 발생건수는 약 11만 건, 2015년은 약 14만 건, 2016년은 15만 건, 2017년은 13만 건으로서 매년 10만 건 이상의 사이버 범죄가 발생하고 있다. 따라서 서비스 제공자가 사용자들의 개인정보를 안전하게 보관하거나, 서비스 이용자인 사용자가 여러 웹사이트에 등록한 아이디/비밀번호를 안전하게 관리하는 것이 중요시되고 있으며, 다양한 보안 솔루션, 안전한 인증 기법 및 인증 프로토콜 등이 필요한 상황이다.

이 논문에서는 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜은 제안한다. 사용자는 로그인을 시도할 때, 아이디, 랜덤챌린지, 디지털인감의 비밀키를 이용하여 일회용 비밀번호인 HOTP Tag를 생성할 수 있으며, 이 Tag를 이용하여 자신이 올바른 사용자라는 것을 인증할 수 있다. 이 프로토콜을 이용하면, 사용자는 비밀번호를 기억할 필요가 없으며, 여러 사이트에 등록되어 있는 여러 계정들을 간편하게 관리할 수 있게 된다. 또한 HOTP Tag는 엔트로피(Entropy)가 높기 때문에[4] 공격자가 쉽게 유추할 수 없으며, 사회공학적 기법으로도 유추하기 힘들다. 이에 따라 사용자는 조금 더 안전하게 온라인 서비스를 사용할 수 있게 된다.

이 논문은 다음과 같이 구성되어 있다. 2장에서는 이전에 연구되어왔던 인증 프로토콜 및 보안 도구 그리고 디지털인감을 소개한다. 3장에서는 제안하는 프로토콜을 설명하고, 4장에서는 프로토콜을 직접 구현하여 실효성을 검증한다. 5장에서는 프로토콜의 성능, 사용성, 보안성을 분석하고, 마지막 6장에서는 결론과 향후 연구에 대해 논의한다.

2. 관련연구

2.1 인증 프로토콜

인증 프로토콜이란, 사용자가 온라인 서비스를 이용하기 위하여 접근 권한을 얻는 절차를 의미한다. 예를 들어, 사용자는 온라인 서비스 제공자와 사전에 비밀번호를 공유하고, 서비스를 이용하고 싶을 때 비밀번호를 이용하여 접근 권한을 얻어 서비스를 이용할 수 있다. 이러한 인증 프로토콜은 로그인 세션 프로토콜, 출석인증 시스템[5] 등의 적용되어 사용되어지고 있다. 초기 인증 프로토콜은 간단하게 비밀번호만을 이용했었지만, 공격자의 비밀번호 탈취 기술이 발전함에 따라 다양한 인증 기법 및 프로토콜이 개발되었다.

사용자가 PC에서 인증을 시도하는 경우에는, 키보드를 입력하는 패턴이 개인마다 다르다는데 기초한 키 입력 패턴 인식(Keystroke dynamics) 기술[6, 7, 8], 키보드를 입력할 때의 발생하는 소리를 이용한 인증 기술[9] 등의 인증 기법 및 프로토콜이 연구되어 왔다. 이러한 인증 기법 및 프로토콜은 PC에서만 사용할 수 있다는 제한이 있으며, 올바른 사용자라고 하더라도 사용자의 상황이나 환경에 의해 인증에 실패할 가능성이 존재한다.

사용자가 스마트폰에서 인증을 시도하는 경우에

는, 검은색과 흰색 키패드를 사용하는 인증 기법[10], 진동을 이용한 인증 기법[11], 키 터치 위치 및 시간과 머신러닝을 이용한 인증 프로토콜[12] 등이 연구되어 왔다. 이러한 기술들은 스마트폰에서만 한정적으로 사용할 수 있다는 단점과 사용자에게 패스워드 뿐만 아니라 색 구분, 기호, 키 터치 위치 및 시간 등도 기억해야한다는 부담이 존재한다.

원패스워드란 사용자가 여러 웹사이트 또는 어플리케이션에 등록해놓은 비밀번호를 관리해주는 비밀번호 통합관리 솔루션[13]이다. 사용자는 웹사이트에 자신의 계정을 등록할 때 원패스워드를 이용하여 복잡한 비밀번호를 생성할 수 있고, 로그인을 시도할 때에는 원패스워드를 이용하여 비밀번호가 자동으로 입력되게 할 수 있다. 그러므로 사용자는 여러 사이트에 등록된 비밀번호를 일일이 관리하지 않아도 된다. 그런데 2015년 소프트웨어 엔지니어인 데일 마이어스는 원패스워드를 사용하던 중 애자일 키체인 파일에 문제가 있다는 것을 인지하였고, 그 결과 사용자가 원패스워드를 어떤 서비스 계정에 사용하는지 등의 개인정보가 유출될 수 있다는 것을 확인하였다[14]. 뿐만 아니라 사용을 위해 서버와 통신을 해야 하는 솔루션이므로 네트워크 경로를 통해 비밀키가 유출될 수 있는 가능성도 존재한다.

2.2 보안 도구

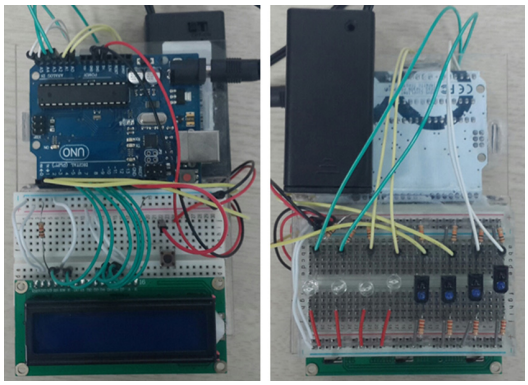
사용자는 로그인을 시도할 때 보안성을 향상시키기 위하여 소프트웨어적인 다양한 인증 기법 및 인증 프로토콜이 아닌, 하드웨어적인 보안 도구를 이용할 수도 있다. OTP(One-Time Password), 보안카드 등은 사용자가 스마트폰, PC 등의 플랫폼 상관없이 사용할 수 있는 하드웨어적인 보안 도구이다. 따라서 사용을 위해서는 OTP 기기 또는 카드 형식으로 제작된 보안 카드를 소지하고 있어야만 한다.

OTP는 무작위로 일회용 비밀번호를 생성하여 인증에 사용한다. 시간 동기화 방식을 사용하는 Time-synchronized OTP, HMAC을 사용하는 HOTP, 서버와 질의 응답 방식을 이용하는 Challenge-Response OTP 등이 있다. 이러한 OTP는 비밀키 관리 문제가 있을 수 있으며, MitM(Man in the Middle), MitB(Man in the Browser)[15]등의 공격으로부터 안전하지 않다.

보안 카드는 4자리 숫자 30여개가 기록되어 있는 난수표이며, 로그인 또는 온라인 금융 거래 시마다 웹사이트에서 요구하는 보안번호를 올바르게 입력함으로서 안전하게 인증을 할 수 있다. 하지만 보안카드의 번호는 고정되어 있으므로 장시간의 스니핑(Sniffing), 피싱(Phishing), 파밍(Pharming) 공격에 취약하다. 또한 사용자가 이미지화하여 스마트폰 등에 저장하고 다닐 경우, 이미지 유출을 통해 보안카드 전체 난수표가 유출될 수 있다는 가능성도 존재한다.

2.3 디지털인감

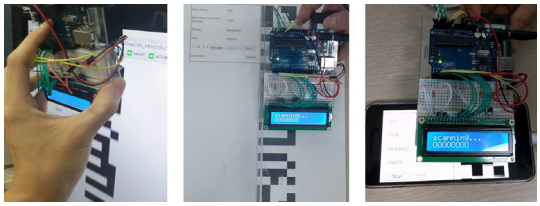
(그림 1)는 아두이노 우노(Arduino UNO)를 이용하여 제작된 디지털인감으로서, 사용자 인증을 위한 데이터를 포함하고 있는 바코드를 스캔하면, 그 데이터와 비밀키 그리고 HOTP 알고리즘을 이용하여 HOTP Tag를 LCD에 출력해주는 보안 도구이다[16].



(그림 1) 디지털인감의 앞면(오른쪽)과 뒷면(왼쪽)

디지털인감은 다음의 (그림 2)와 같이, 모니터 스크린에 있는 바코드와 실제 종이에 출력된 바코

드를 모두 스캔할 수 있기 때문에 온라인, 오프라인에 사용할 수 있으며, 따라서 스마트폰, PC 등과 같은 플랫폼과 상관없이 사용될 수 있다.



(그림 2) 디지털인감의 사용 예

종이가 아닌, 스마트폰, PC 등과 같은 온라인 플랫폼에서 사용하는 경우에는, 바코드 제공자가 바코드를 자동적으로 스크롤 되게 제작할 수 있고, 사용자는 디지털인감을 모니터 스크린에 가져다대기만 하면 자동적으로 스캔이 되며, 따라서 사용자는 간편하게 스캔을 할 수 있다. 디지털인감은 로그인, 온라인 뱅킹, 모바일 뱅킹, IoT 키 분배 등의 다양한 인증 프로토콜에 적용될 수 있으며 HMAC 알고리즘을 이용한 HOTP를 사용하기 때문에 MitM, MitB 공격 등에 강하며, 사용할 때에는 USB 또는 네트워크에 연결할 필요가 없으므로 비밀키 관리에도 안전하다고 할 수 있다.

3. 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜

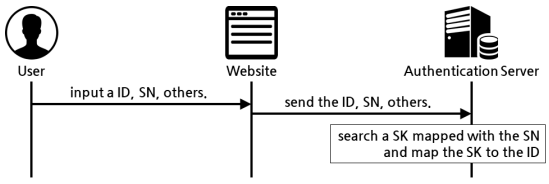
이 논문에서는 디지털인감을 아이디/패스워드 로그인 인증 시스템에 적용한 프로토콜을 제안한다. 이 프로토콜은 디지털인감의 비밀키가 인증 서버에 저장되어 있는 프로토콜과, 인증 서버에 저장되어 있지 않은 프로토콜로 분류할 수 있다. 비밀키가 인증 서버에 저장되어 있는 경우는 상대적으로 사용성을 강조한 프로토콜이며, 저장되어 있지 않은 경우는 상대적으로 보안성을 강조한 프로토콜이다.

3.1 비밀키가 인증 서버에 저장되어 있는 프로토콜

이 프로토콜은 회원 가입 단계, 로그인 단계로 구성되어 있으며, 다음과 같이 세 가지 사항을 가정한다. (1) 사용자는 인증 서버를 관리하는 기관으로부터 고유의 시리얼넘버가 부여되고 시리얼넘버와 1:1로 매핑(저장)되어 있는 비밀키와 HOTP 알고리즘이 내장된 디지털인감을 발급 받았다. (2) 인증 서버는 내부 데이터베이스에 사용자에게 발급한 디지털인감의 비밀키를 안전하게 저장하고 있으며, HOTP 알고리즘을 사용할 수 있다. (3) 사용자가 로그인하는 웹사이트는 안전하게 인증 서버와 연결되어 있다.

3.1.1 회원 가입 단계

사용자는 웹사이트에서 회원 가입을 할 때, 아이디를 설정하고 소유하고 있는 디지털인감의 시리얼넘버와 다른 기타 정보를 입력한다. 이때, 비밀번호 설정은 요구되지 않는다. 웹사이트는 아이디와 시리얼넘버를 인증 서버로 전송한다. 인증 서버는 입력받은 시리얼넘버와 매핑되어 있는 비밀키를 검색하여 아이디와 매핑시킨다. 이 과정은 사용자와 인증 서버가 안전하게 비밀키를 공유하는 것을 의미한다. 이 과정이 완료되면 회원 가입이 완료된다. 이 단계를 도식화하여 표현하면 다음의 (그림 3)과 같다.



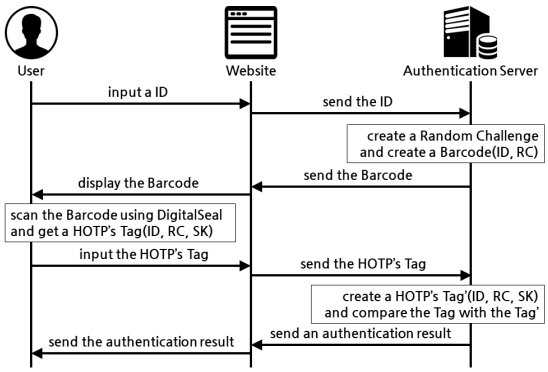
(그림 3) 비밀키가 인증 서버에 저장되어 있는 프로토콜의 회원 가입 단계

3.1.2 로그인 단계

사용자는 웹사이트에 로그인하기 위하여 아이디를 입력하고, 웹사이트는 아이디를 인증 서버로 전송한다. 인증 서버는 랜덤챌린지를 생성한 다음 입력받은 아이디와 결합하여 바코드를 생성하고, 웹사이트에 전송한다. 웹사이트는 인증 서버로부터 전송받은 바코드를 사용자에게 출력해주고, 사용자는 자신이 소유하고 있는 디지털인감으로 바코드를 스캔한다. 디지털인감은 아이디와 랜덤챌린지로 구

성된 바코드 데이터, 내장된 비밀키 그리고 HOTP 알고리즘으로 HOTP Tag를 생성하여 LCD에 출력한다. 사용자는 디지털인감 LCD에 출력된 HOTP Tag를 비밀번호로서 웹사이트에 입력한다.

웹사이트는 사용자로부터 입력받은 HOTP Tag를 인증 서버로 전송하고, 인증 서버는 이전에 입력받은 아이디, 생성한 랜덤챌린지, 미리 공유된 비밀키와 HOTP 알고리즘을 사용하여 HOTP Tag`을 생성한다. 그리고 사용자로부터 입력받은 HOTP Tag와 직접 생성한 HOTP Tag`을 비교한다. 만약 HOTP Tag와 HOTP Tag`이 동일하다면, 로그인을 시도한 사용자가 자신이 입력한 아이디와 매핑되어있는 비밀키를 공유하고 있는 올바른 사용자라는 것이 증명되기 때문에, 인증 서버는 사용자에게 서비스 접근 권한을 허가하고, 그렇지 않으면 허가하지 않는다. 이 단계를 도식화하여 표현하면 다음의 (그림 4)과 같다.



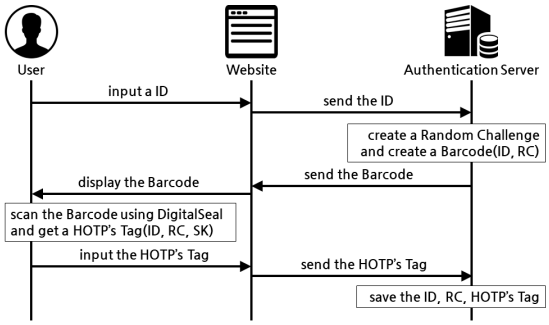
(그림 4) 비밀키가 인증 서버에 저장되어 있는 프로토콜의 로그인 단계

3.2 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜

이 프로토콜은 회원 가입 단계, 로그인 단계, 비밀번호 재설정 단계로 구성되어 있으며, 다음과 같이 두 가지 사항을 가정한다. (1) 사용자는 인증 서버를 관리하는 기관으로부터 고유의 비밀키와 HOTP 알고리즘이 내장된 디지털인감을 발급 받았다. (2) 사용자가 로그인하는 웹사이트는 안전하게 인증 서버와 연결되어 있다.

3.2.1 회원 가입 단계

사용자는 웹사이트에서 회원 가입을 할 때 아이디를 설정한다. 웹사이트는 아이디를 인증 서버로 전송하고, 인증 서버는 랜덤챌린지를 생성한 후 아이디와 결합하여 바코드를 생성한 다음 웹사이트로 전송한다. 웹 사이트는 인증 서버로부터 받은 바코드를 사용자에게 출력해준다. 사용자는 자신이 소유하고 있는 디지털인감으로 바코드를 스캔한다. 디지털인감은 아이디와 랜덤챌린지로 구성되어 있는 바코드 데이터, 내장된 비밀키 그리고 HOTP 알고리즘으로 HOTP Tag를 생성하여 LCD에 출력한다. 사용자는 디지털인감 LCD에 출력된 HOTP Tag를 웹사이트에 입력한다. 웹사이트는 사용자가 입력한 HOTP Tag를 인증 서버로 전송한다. 인증 서버는 아이디, 랜덤챌린지, HOTP Tag를 저장하고, 저장이 완료되면 회원 가입이 완료된다. 이때, 이 단계에서 비밀번호 설정은 요구되지 않는다. 이 단계를 도식화하여 표현하면 다음의 (그림 5)과 같다.



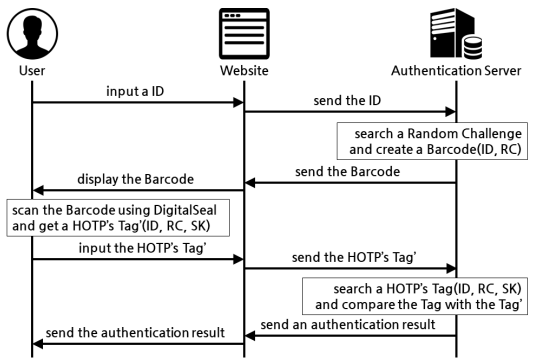
(그림 5) 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜의 회원 가입 단계

3.2.2 로그인 단계

사용자는 웹사이트에 로그인하기 위하여 아이디를 입력하고, 웹사이트는 아이디를 인증 서버로 전송한다. 인증 서버는 입력받은 아이디와 매핑되어 있는 랜덤챌린지를 이용하여 바코드를 생성하여, 웹사이트에 전송한다. 웹사이트는 바코드를 사용자에게 출력해주고, 사용자는 자신이 소유하고 있는 디

지털인감으로 바코드를 스캔하면, 디지털인감은 아이디와 랜덤챌린지로 구성된 바코드 데이터, 내장된 비밀키 그리고 HOTP 알고리즘으로 HOTP Tag`을 생성하여 LCD에 출력한다. 사용자는 생성된 HOTP Tag`를 비밀번호로서 웹사이트에 입력하고, 웹사이트는 인증 서버로 HOTP Tag`를 전송한다.

인증 서버는 기존에 저장되어 있던 사용자의 HOTP Tag와 전송 받은 HOTP Tag`을 비교한다. 만약 HOTP Tag와 HOTP Tag`이 동일하다면, 로그인을 시도한 사용자가 자신이 입력한 아이디에 매핑되어 있는 HOTP Tag와 같은 HOTP Tag`을 생성했다는 것이기 때문에, 올바른 사용자라는 것이 증명된다. 다음으로 인증 서버는 사용자에게 서비스 접근 권한을 허가하고, 그렇지 않으면 허가하지 않는다. 이 단계를 도식화하여 표현하면 다음의 (그림 6)과 같다.

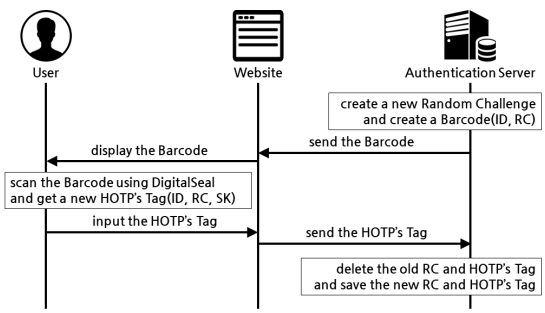


(그림 6) 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜의 로그인 단계

3.2.3 비밀번호 재설정 단계

비밀키가 인증 서버에 저장되어 있는 프로토콜은 사용자가 로그인을 시도할 때마다, 인증 서버는 매번 새로운 랜덤챌린지를 생성하여 사용한다. 그로 인해 HOTP Tag과 HOTP Tag`이 매번 변경되기 때문에, 매번 다른 비밀번호를 사용하게 된다. 그런데 이 프로토콜은 사용자가 로그인을 시도할 때, 이전에 저장되어 있는 랜덤챌린지를 사용하기 때문에 매번 변경되지 않는 HOTP Tag와 HOTP Tag`이 사용되고, 그로인해 고정된 비밀번호를 사용하게 된다. 이를 해결하기 위해 비밀번호 재설정 단계가 요구된다.

사용자가 로그인에 성공하면 인증 서버는 새로운 랜덤챌린지를 생성한다. 그리고 아이디와 결합하여 새로운 바코드를 생성한 후 웹사이트에 전송한다. 웹사이트는 전송받은 바코드를 사용자에게 출력해 주고, 사용자는 자신이 소유하고 있는 디지털인감으로 바코드를 스캔한다. 스캔 후, 사용자가 디지털인감에 출력된 HOTP Tag를 확인하고 웹사이트에 입력하면 웹사이트는 인증 서버로 전송한다. 인증 서버는 기존에 아이디와 매핑되어 있는 랜덤챌린지와 HOTP Tag를 삭제하고, 새로운 랜덤챌린지와 HOTP Tag를 저장한다. 이렇게 저장된 랜덤챌린지와 HOTP Tag는 다음번 로그인에 사용되며, 로그인 할 때마다 이 단계가 반복되어 매번 저장된 랜덤챌린지와 HOTP Tag는 매번 새로운 것으로 변경된다. 그에 따라 사용자는 매번 변경된 비밀번호를 사용할 수 있게 된다. 이 단계를 도식화하여 표현하면 다음의 (그림 7)과 같다.



(그림 7) 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜의 비밀번호 재설정 단계

4. 구현

이 논문에서 제안하는 인증 프로토콜의 실효성을 검증하기 위하여, 디지털인감이 소개되어 있는 논문[16]의 디지털인감과 바코드를 제안하는 인증 프로토콜에 적합하게 재구현하였고, 웹사이트와 인증 서버를 직접 구현하였다.

디지털인감은 영문 3글자와 숫자 7글자를 의미

하는 바코드를 스캔하여 HOTP Tag를 생성할 수 있으므로, 우리는 영문 아이디 첫 3글자, 랜덤챌린지 숫자 7글자를 포함하는 바코드를 스캔하여 디지털인감 LCD에 출력하도록 재구현하였다. 그에 따라 바코드는 사용자의 영문 아이디 첫 3글자와 인증 서버에서 만들어진 랜덤챌린지 숫자 7글자를 이용하여 생성되게 재구현하였다.

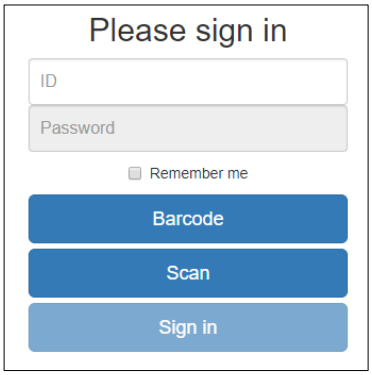
웹사이트는 윈도우 환경에서 HTML, Javascript를 이용하여, 인증 서버는 리눅스 환경에서 Python을 이용하여, 웹사이트와 인증 서버의 통신은 TCP/IP 소켓 프로그래밍을 통해 구현하였다.

4.1 비밀키가 인증 서버에 저장되어 있는 프로토콜

이 섹션에서는 3.1에서 가정한 3가지 사항에 대하여 똑같이 가정한다. 즉, 사용자는 디지털인감을 발급 받았고, 인증 서버는 비밀키를 안전하게 보관하며, 웹사이트와 안전하게 연결되어 있다는 것을 가정한다.

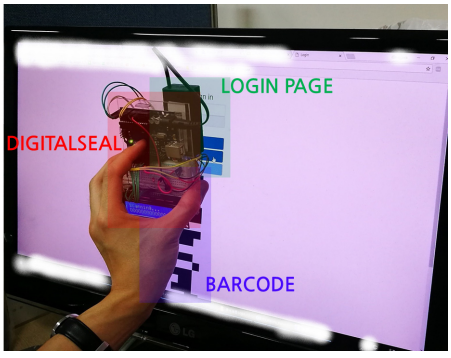
사용자는 웹사이트에 회원 가입을 하기 위해 아이디 'jcptk677'을 입력하고, 사전에 발급받은 디지털인감의 시리얼넘버와 다른 기타 정보를 입력한다. 웹사이트는 사용자의 정보를 인증 서버에 전달하고, 인증 서버는 입력받은 시리얼넘버와 매핑되어 있는 비밀키를 검색하여 아이디와 매핑시킨다. 이를 통해 사용자와 인증 서버는 비밀키를 안전하게 공유하게 되고, 회원 가입 단계는 완료된다.

(그림 8)는 비밀키가 인증 서버에 저장되어 있는 프로토콜의 실효성을 검증하기 위하여 구현한 웹사이트의 로그인 페이지이다.



(그림 8) 실효성 검증을 위해 구현한 웹사이트의 로그인 페이지

사용자가 아이디 'jcptk677'을 입력한 뒤 Barcode 버튼을 클릭하면, 인증 서버는 숫자 7자리의 랜덤챌린지 '1630420'을 생성하고 사용자로부터 입력받은 영문 아이디의 첫 3글자와 결합하여 바코드를 생성한 다음 웹사이트에 전송한다. 웹사이트는 사용자에게 바코드를 출력해주고, 사용자는 바코드 첫 라인에 디지털인감을 가져다 놓는다. 그리고 Scan 버튼을 클릭하면 (그림 9)처럼 바코드는 자동적으로 0.1초에 한 라인씩 위로 스크롤되며, 디지털인감은 바코드를 스캔하게 된다.



(그림 9) 디지털인감으로 바코드를 스캔하면 장면

스캔이 완료 되면 웹페이지에서의 Password 입력 부분과 Sign in 버튼이 활성화되고, (그림 10)처럼 디지털인감의 LCD에는 HOTP Tag 'e482b77f57'이 출력된다.

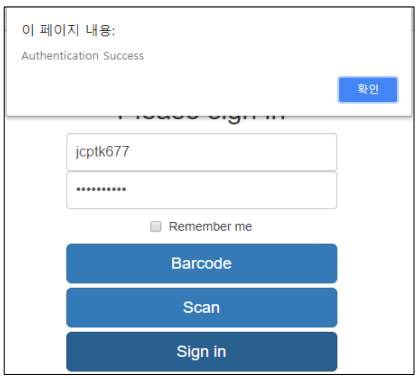
(그림 10) 스캔이 완료된 후의 디지털인감

사용자는 자신의 아이디의 영문 첫 3글자와 랜덤 챌린지로 바코드가 생성되었는지 확인을 하고, 그에 따라 생성된 HOTP Tag를 Password 입력 부분에 입력한 다음 Sign in 버튼을 클릭한다. HOTP Tag는 인증 서버로 전송이 되고, 인증 서버는 아이디, 랜덤챌린지, 비밀키로 HOTP Tag`을 생성한다. 그리고 전송받은 HOTP Tag와 비교한다. 만약 동일하다면 사용자에게 (그림 11)처럼 인증 성공을 리턴한다.

```
HOTP Tag from client: e482b77f57

ID: jcp
RC: 1630420
SK: 123456789

creates a HOTP Tag' using ID, RC, SK
HOTP Tag' = HMAC(ID, RC, SK) = e482b77f57
compares the HOTP Tag with the HOTP Tag'

Authentication Success
```

(그림 11) 인증 서버에서의 사용자 인증 결과

사용자는 (그림 12)처럼 인증 성공이라는 메시지를 받고 로그인이 완료된다.



(그림 12) 웹사이트에서의 사용자 인증 결과

결과적으로 구현 결과에 이상이 없었으며, 제안한 프로토콜이 실제로 활용될 수 있다는 것을 확인할 수 있었다.

4.2 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜

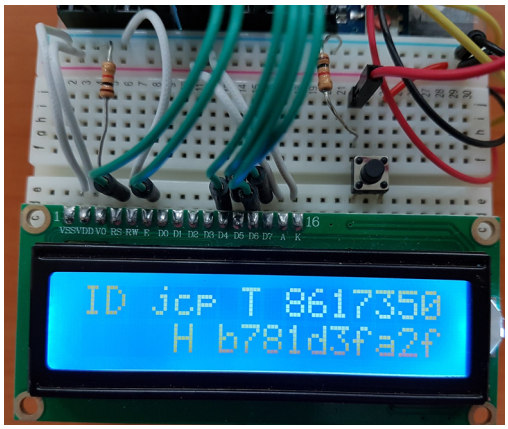
이 섹션에서는 3.2에서 가정한 2가지 사항에 대하여 똑같이 가정한다. 즉, 사용자는 디지털인감을 발급 받았고, 웹사이트와 안전하게 연결되어 있다는 것을 가정한다.

사용자는 회원 가입을 위해 웹사이트에 접속하여 아이디 'jcptk677'을 입력한다. 웹사이트는 인증 서버로 아이디를 전송하고, 인증 서버는 랜덤챌린지 '1630420'을 생성하고 사용자로부터 받은 아이디와 결합하여 바코드를 생성한다. 웹사이트는 인증 서버로부터 바코드를 받아서 사용자에게 출력해준다. 사용자는 발급받은 자신의 디지털인감으로 바코드를 스캔하여 HOTP Tag 'e482b77f57'를 생성하고, 입력한다. 인증 서버는 사용자의 HOTP Tag를 안전하게 저장 및 보관한다. 이를 통해 사용자의 HOTP Tag는 인증 서버에 안전하게 저장이 되었고, 회원 가입 단계는 완료된다.

사용자가 로그인 페이지에서 아이디 'jcptk677'을 입력한 뒤 Barcode 버튼을 클릭하면, 인증 서버는 아이디와 매핑되어 있는 랜덤챌린지를 검색한 후 사용자가 입력한 아이디의 첫 3글자와 결합하여

바코드를 생성한 다음 웹사이트에 전송한다. 웹사이트는 사용자에게 바코드를 출력해주고, 사용자는 바코드 첫 라인에 디지털인감을 가져다 놓는다. 그리고 Scan 버튼을 클릭하면 바코드는 자동적으로 0.1초에 한 라인씩 위로 스크롤되며, 디지털인감은 바코드를 스캔하게 된다. 스캔이 완료되면 웹페이지에서의 Password 입력 부분과 Sign in 버튼이 활성화된다. 사용자는 디지털인감의 LCD를 통해 자신의 아이디의 영문 첫 3글자와 랜덤챌린지로 바코드가 생성되었는지 확인을 하고, 그에 따라 생성된 HOTP Tag` 'e482b77f57' 을 Password 입력 부분에 입력한 다음 Sign in 버튼을 클릭한다. 인증서버는 사용자로부터 전송받은 아이디로 저장되어 있는 HOTP Tag 'e482b77f57' 을 검색한 후, 입력받은 HOTP Tag` 'e482b77f57' 과 비교하여 동일하다면 로그인 성공을 사용자에게 리턴해준다.

로그인 완료 후 인증 서버는 새로운 랜덤챌린지 '8617350' 을 생성한 후 사용자의 아이디와 결합하여 새로운 바코드를 사용자에게 출력해준다. 사용자는 자신의 디지털인감으로 바코드를 스캔하고, 스캔이 완료된 후 디지털인감의 LCD를 통해 (그림 13)와 같이 자신의 아이디와 새로운 랜덤챌린지로 만들어진 새로운 HOTP Tag 'b781d3fa2f' 를 확인하고, 인증서버 HOTP Tag를 입력한다.



(그림 13) 비밀번호 재설정 단계에서 생성된 새로운 HOTP Tag

인증 서버는 (그림 14)과 같이 기존에 저장하고 있던 랜덤챌린지와 HOTP Tag 'e482b77f57' 을 삭제하고, 사용자로부터 입력받은 새로운 랜덤챌린지와 HOTP Tag 'b781d3fa2f' 를 저장한다. 이렇게 저장된 HOTP Tag는 다음번 로그인 때 사용된다.

```
HOTP Tag from client: b781d3fa2f

deletes the old RC and HOTP Tag
saves the new RC and HOTP Tag

ID: jcp
RC: 8617350
Tag: b781d3fa2f
```

(그림 14) 비밀번호 재설정 단계에서 저장된 새로운 랜덤챌린지와 HOTP Tag

결과적으로 구현 결과에 이상이 없었으며, 제안한 프로토콜이 실제로 활용될 수 있다는 것을 확인할 수 있었다.

5. 성능, 사용성, 보안성 분석

5.1 제안하는 프로토콜의 성능 분석

제안하는 프로토콜에서 디지털인감은 아두이노 우노로 제작되었으며, 아두이노 우노는 6개의 아날로그 입력 핀, 14개의 디지털 입·출력 핀, 32KB Flash Memory, 2KB SRAM, 1KB EEPROM 등으로 구성되어 있다. 이렇게 작은 컴퓨팅 파워와 용량을 가지고 있지만, HOTP 알고리즘의 사용, 비밀키 내장, 스캔을 위한 다양한 센서의 입·출력 그리고 LCD에 계산된 HOTP Tag를 출력하기에는 충분하다. 왜냐하면 HOTP Tag는 스캔 후 0.1초 내에 계산 및 생성되어 1602 LCD에 출력되며, 따라서 사용자에게 큰 불편함을 초래하지 않기 때문이다.

구현 단계에서 사용된 웹사이트를 제작한 클라이언트용 데스크탑의 스펙은 16GB Memory, 256GB SSD, 윈도우 10이었으며, 인증 서버의 스펙은 8GB Memory, 100GB HDD, Ubuntu Linux 16.04였다. 구현한 프로토콜에서 웹사이트와 인증

서버간의 통신 그리고 인증 서버에서 이루어지는 연산들인 바코드 생성, 바코드 전송, HOTP Tag 전송, Tag와 Tag` 비교, 인증 결과 전송은 모두 0.1초 내에 완료되었기 때문에, 사용자에게 큰 불편함을 초래하지 않았다.

5.2 제안하는 프로토콜의 사용성 분석

제안하는 프로토콜인, 디지털인감을 이용한 비밀번호 인증 프로토콜은 로그인을 할 때마다 비밀번호가 변경되며, 사용자는 디지털인감을 통해 비밀번호 역할을 하는 HOTP Tag를 확인할 수 있다. 그러므로 사용자는 비밀번호를 기억할 필요가 없으며, 여러 사이트의 비밀번호를 관리할 필요가 없어진다. HOTP Tag는 사용자의 아이디, 랜덤챌린지 그리고 사용자의 디지털인감으로 매번 다르게 생성되기 때문이다.

디지털인감이 소개되어 있는 논문[16]의 사용자 실험 결과를 확인하면, 디지털인감으로 모니터의 바코드를 스캔하는 시간은 2.6초이다. 비밀키가 인증 서버에 저장되어 있는 프로토콜에서는 스캔을 한 번만 하면 되고, 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜에서는 스캔을 두 번만 하면 되므로, 사용하기에 어려움이 많지 않고, 시간이 오래 걸리지 않는다는 것을 확인할 수 있었다.

기존에 연구되어 왔던 키 입력 패턴 인식, 스마트폰에서 진동을 이용한 인증 방법 등의 다양한 인증 기법 및 프로토콜은 플랫폼에 제한적이었으나, 제안하는 프로토콜은 플랫폼에 상관없이 어디에나 적용하여 사용이 가능하다.

기존에 사용되어지고 있는 Time-synchronized OTP, HOTP, Challenge-Response OTP, 보안카드 등의 보안 도구는 비밀번호와 함께 사용해야 하기 때문에 2-FACTOR 인증인 반면, 제안하는 프로토콜은 1-FACTOR 인증이기 때문에 더 간편한 인증 프로토콜이라는 것을 확인할 수 있었다.

5.3 제안하는 프로토콜의 보안성 분석

비밀키가 서버에 저장되어 있는 프로토콜은 회원가입 단계와 로그인 단계로 이루어져 있다.

회원 가입 단계는 사용자와 인증서버 간의 비밀키 공유를 목표로 하는데, 이 작업은 HOTP 알고리즘을 사용하여 MitM, MitB 공격을 방어하기 위함이다.

로그인 단계에서는 사용자가 바코드를 스캔 후 생성된 HOTP Tag를 비밀번호로 입력하여 안전한 로그인을 목표로 하고 있다. 이 단계에서 바코드는 인증 서버가 생성한 랜덤챌린지를 포함하고 있는데, 이것은 일회용 비밀번호의 특징을 부여하기 때문에, 스니핑, 키로깅, 숄더서핑 공격으로 인해 사용된 HOTP Tag가 유출되어도 재사용될 수 없다는 효과를 소유하게 해준다. 또한 이러한 특징으로 사용자는 여러 사이트에 비밀번호를 각각 다르게 설정하는 것과 같은 효과를 획득할 수 있고, 따라서 향상된 보안성을 가질 수 있다. 사용자가 바코드를 스캔하기 위하여 디지털인감을 사용할 때에는 네트워크에 연결하거나 USB에 연결하여 사용하지 않아도 되므로 공격자는 디지털인감에 내장되어 있는 비밀키를 탈취할 수 없다. 공격자가 침투할 수 있는 경로가 존재하지 않기 때문이다. 따라서 비밀키는 외부로부터 안전하게 보관된다. 바코드를 스캔한 이후에 생성되는 HOTP Tag는 엔트로피가 높기 때문에 공격자가 쉽게 유추할 수 없다. 또한 사용자와 비밀번호간의 관계성이 낮으므로 사용자는 공격자의 사회공학적 공격 기법으로부터 안전해질 수 있다.

비밀키가 서버에 저장되어 있지 않은 프로토콜은 회원 가입 단계, 로그인 단계, 비밀번호 재설정 단계로 구성되어 있다.

회원 가입 단계에서는 HOTP Tag를 공유하는 것을 목표로 하며, 이 작업은 HOTP 알고리즘을 사용하여 MitM, MitB 공격을 방어하기 위함이다. 또한 랜덤챌린지가 포함된 바코드를 사용하기 때문에 일회용 비밀번호의 특징을 부여하며, 그로인해 스니핑, 키로깅, 숄더서핑 공격으로인 해 사용된 HOTP Tag가 유출되어도 재사용될 수 없다는 효과를 소유하게 해준다. 뿐만 아니라 이러한 특징으로 사용자는 여러 사이트에 비밀번호를 각각 달게

설정하는 것과 같은 효과를 획득할 수 있고, 따라서 향상된 보안성을 가질 수 있다.

로그인 단계에서는 사용자가 바코드를 스캔 후 생성된 HOTP Tag를 비밀번호로 입력하여 안전한 로그인을 목표로 하고 있다. 사용자가 바코드를 스캔하기 위하여 디지털인감을 사용할 때에는 네트워크에 연결하거나 USB에 연결하여 사용하지 않아도 되므로 공격자는 디지털인감에 내장되어 있는 비밀키를 탈취할 수 없다. 공격자가 침투할 수 있는 경로가 존재하지 않기 때문이다. 따라서 비밀키는 외부로부터 안전하게 보관된다. 바코드를 스캔한 이후에 생성되는 HOTP Tag는 엔트로피가 높기 때문에 공격자가 쉽게 유추할 수 없다. 또한 사용자와 비밀번호간의 관계성이 낮으므로 사용자는 공격자의 사회공학적 공격 기법으로부터 안전해질 수 있다.

비밀번호 재설정 단계에서는 새로운 랜덤챌린지로 생성된 HOTP Tag를 인증 서버에 저장하는 작업이며, 회원 가입 단계와 같이, MitM 및 MitB 방어, HOTP Tag 유출 방어, 비밀번호 피로(Password Fatigue)의 해결 등의 이점을 취할 수 있다.

기존에 연구되어 왔던 키 입력 패턴 인식, 스마트폰에서 진동을 이용한 인증 방법 등의 다양한 인증 기법 및 프로토콜은 사용자의 비밀번호 또는 사용자의 패턴 입력 특징이 스니핑, 키로깅, 숄더서핑 등으로 유출되었을 때 보안 사고를 야기할 수 있지만, 제안하는 프로토콜은 유출이 되어도 One-Time Password 특징을 가지고 있기 때문에, 유출된 비밀번호를 다시 사용할 수 없다. 그리고 원패스워드는 소프트웨어 솔루션이므로 비밀키 관리에 취약할 수 있지만, 제안하는 프로토콜에서는 디지털인감이 안전하게 비밀키를 보관하므로, 비밀키 관리에 있어서 더 향상된 보안성을 가질 수 있다.

기존에 사용되어 지고 있는 Time-synchronized OTP는 시간차 공격에 취약하고, 엔티티(Entity) 기반 인증이므로 MitM, MitB 공격에 취약하다[15]. HOTP는 사용할 때 네트워크에 연결되어 있는 스마트폰의 어플리케이션 또는 PC의 어플리케이션이 필요하므로, 비밀키 관리에 문제가 있을 수 있다. 공격자가 비밀키를 탈취할 수 있는 경로가 존재하기 때문이다. Challenge-Response OTP는 Exhaustive Key Search 공격에 취약하며, 스마트폰 또는 PC에서 Response를 하게 되면 HOTP와 같이 비밀키 관리에 문제가 있을 수 있다. 보안카드는 랜덤한 수가 제한적이므로 장기간 스니핑 등에 취약하고, 보안카드를 스마트폰에 이미지로 저장하여 사용하는 경우에는 이미지 유출을 통해 보안카드 전체가 유출 될 수 있는 가능성도 존재한다.

이렇게 기존에 존재하는 여러 OTP들은 다양한 취약점이 존재하는데, 제안하는 프로토콜은 HOTP를 이용하기 때문에 MitM, MitB 등의 공격을 방어할 수 있고, 네트워크 또는 USB 연결이 필요 없는 디지털인감 내부에 비밀키를 안전하게 보관하고 있기 때문에 비밀키 관리에 문제를 해결할 수 있다. 또한 사용될 수 있는 HOTP Tag의 수가 제한적이지 않기 때문에 보안카드보다 더 안전하다고 말할 수 있다.

6. 결론

이 논문에서는 디지털인감을 이용한 안전한 비밀번호 인증 프로토콜을 제안하였다. 이 프로토콜은 비밀키가 인증 서버에 저장되어 있는 프로토콜과 비밀키가 인증 서버에 저장되어 있지 않은 프로토콜로 분류할 수 있다. 비밀키가 인증 서버에 저장되어 있는 경우는 상대적으로 사용성을 강조한 프로토콜이며, 저장되어 있지 않은 경우는 상대적으로 보안성을 강조한 프로토콜이다. 사용자가 이 프로토콜을 이용하면, 자신의 디지털인감으로 바코드를 스캔하는 작업을 통해 안전한 일회용 비밀번호를 인증에 사용할 수 있다. 결과적으로 비밀번호를 기억하지 않아도 되며, 여러 웹사이트에 등록되어 있는 여러 계정들의 비밀번호를 일일이 관리하지 않아도 된다. 또한 스니핑, 키로깅, 숄더서핑, MitM, MitB, 사회공학적 공격으로부터 안전할 수 있고, 안전하게 비밀키를 보관할 수 있으므로 기존 솔루션보다 보안성이 향상된 인증 프로토콜을 사용할 수

있다.

디지털인감의 소형화, 스캔 정확도, 스캔 소요시간 감소 등의 연구는 추후 연구 주제로 남기며, 디지털인감을 IoT[17] 인증, 웨어러블 헬스케어[18] 인증 등 다양한 분야에 적용시키는 연구도 추후 연구 주제로 남긴다.

Acknowledgements

이 논문은 2016년도 정부(과학기술정보통신부)의 재원으로 한국연구재단-글로벌연구실사업의 지원을 받아 수행된 연구임(NRF-2016K1A1A2912757).

참고문헌

〔1〕 윤성관, 송윤정, "2017년중 국내 인터넷뱅킹서비스 이용현황", 한국은행 보도자료, 2018.

〔2〕 장민지, "2017 대한민국 게임백서 요약본", 한국콘텐츠진흥원 보도자료, 2017.

〔3〕 "전체 사이버범죄 발생 및 검거 현황", 경찰청, 2018.

〔5〕 이재홍, 채건희, 임근영, 설지환, 최성민, 임성욱, "비콘과 생채인식을 결합한 출석인증 시스템", 한국차세대컴퓨팅학회 논문지, 14권, 2호, pp.24-32, 2018, 4.

〔4〕 F. Hoornaert, D. Naccache, O. Ranen, D. M'Raihi, M. Bellare, "Hotp: An hmac-based one-time password algorithm.", RFC4226, 1997.

〔6〕 Lívia C. F. Araujo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga, Lee L. Ling, and João B. T. Yabu-uti, "User Authentication Through Typing Biometrics Features", IEEE Transactions on Signal Processing, Vol.53, No.2, pp.851-855, 2005.

〔7〕 P. Panasiuk and K. Saeed, "A Modified Algorithm for User Identification by His Typing on the Keyboard", Image Processing and Communications Challenges 2, Springer, Berlin, Heidelberg, pp.113-120, 2010.

〔8〕 S. J. Shepherd, "Continuous authentication by analysis of keyboard typing characteristics", Security and Detection 1995, May. 1995.

〔9〕 Joseph Roth, Xiaoming Liu, Arun Ross, Dimitris Metaxas, "Biometric authentication via keystroke sound", 2013 International Conference on Biometrics (ICB), June, 2013.

〔10〕 V. Roth, K. Richter, and R. Freidinger, "A PIN-Entry Method Resilient Against Shoulder Surfing", CCS '04 Proceedings of the 11th ACM conference on Computer and Communications Security, Washington, pp.236-245, 2004.

〔11〕 송정은, 김진복, 이문규, "진동을 이용한 스마트 디바이스 사용자 인증 방법", 한국차세대컴퓨팅학회 논문지, 10권, 11호, pp.6-21, 2014, 2.

〔12〕 정창훈, Zayabaatar Dagvatur, 장룡호, 양대헌, 이경희, "머신러닝을 이용한 사용자 행동 인식 기반의 PIN 입력 기법 연구", 한국정보처리학회 컴퓨터 및 통신시스템 논문지, 7권, 5호, pp-127-136, 2018, 5.

〔13〕 1password, https://1password.com/

〔14〕 Dale Myers, "1Password Leaks Your Data", https://myers.io/2015/10/22/1password-leaks-your-data/

〔15〕 맹영재, 신동오, 김성호, 양대헌, 이문규, "국내 인터넷뱅킹 계좌이체에 대한 MITB 취약점 분석," Internet and Information Security, 한국인터넷진흥원, 1권, 2호, pp.101-118, 2010, 11.

〔16〕 ChangHun Jung, Jeonil Kang, Aziz Mohaisen, and DaeHun Nyang, "DIGITALSEAL: A TRANSACTION AUTHENTICATION TOOL FOR ONLINE AND OFFLINE TRANSACTIONS", Proceedings of 2018 IEEE International Conference on Acoustics, Speech and Signal Processing(ICASSP), Apr. 2018.

〔17〕 임철수, "IoT 서비스 활용사례 분석 및 산업 활성화 이슈", 한국차세대컴퓨팅학회 논문지, 11권, 6호, pp.41-50, 2015, 12.
〔18〕 임철수, "헬스밴드 주요기술 이슈 및 제품별 사용자 경험 분석", 한국차세대컴퓨팅학회 논문지, 14권, 3호, pp.25-33, 2018, 6.

저자소개

◆ 정창훈

- 2014년 2월 인하공업전문대학 컴퓨터시스템과 졸업
- 2014년 8월 국가평생교육진흥원 컴퓨터공학과 졸업
- 2017년 2월 인하대학교 컴퓨터정보공학과 석사
- 2017년 3월~현재 인하대학교 컴퓨터공학과 박사과정
- 관심분야: 인증 프로토콜, 네트워크 보안, 정보보호

◆ 민대홍

- 2017년 2월 인하대학교 수학과 졸업
- 2017년 3월~현재 인하대학교 컴퓨터공학과 통합과정
- 관심분야: 네트워크 보안, 알고리즘, 인증 프로토콜

◆ 양대헌

- 1994년 2월 한국과학기술원 과학기술대학 전기 및 전자공학과 졸업
- 1996년 2월 연세대학교 컴퓨터과학과 석사
- 2000년 8월 연세대학교 컴퓨터과학과 박사
- 2000년 9월~2003년 2월 한국전자통신연구원 정보보호연구본부 선임연구원
- 2003년 2월~현재 인하대학교 컴퓨터공학과 교수
- 관심분야: 암호이론, 암호프로토콜, 인증 프로토콜, 무선 인터넷 보안, 네트워크 보안

◆ 이경희

- 1993년 2월 연세대학교 컴퓨터 과학과 석사
- 1998년 8월 연세대학교 컴퓨터 과학과 석사
- 2004년 2월 연세대학교 컴퓨터 과학과 박사
- 1993년 1월~1996년 5월 LG소프트(주) 연구원
- 2000년 12월~2005년 2월 한국전자통신연구원 선임연구원
- 2005년 3월~현재 수원대학교 전기공학과 부교수
- 관심분야: 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식