http://dx.doi.org/10.7840/kics.2014.39B.4.207

웹 서비스를 위한 QR 코드 기반 상호 인증 시스템

박 지 예◆, 김 정 인*, 신 민 수*, 강 남 희°

QR-Code Based Mutual Authentication System for Web Service

Ji-ye Park◆, Jung-in Kim*, Min-su Shin*, Namhi Kang°

요 약

많은 웹 서비스에서 편리성을 이유로 패스워드 기반 인증 시스템을 주로 사용한다. 패스워드 기반 인증 시스템은 패스워드 추측공격, 사전식 대입공격, 키 로깅 공격 등 다양한 공격에 취약한 것으로 알려져 왔다. 뿐만 아니라 대부분 웹 기반 인증 시스템은 서버가 사용자를 인증하는 단방향 인증만을 제공하므로 사용자는 현재 접속하여 비밀 정보를 남기고자하는 서버가 적합한지 검증 할 수 없다. 따라서 DNS 스푸핑 공격이나 피싱, 파밍과 같은 공격에 대응하기가 어렵다. 이러한 웹 서비스의 보안 취약점을 개선하기 위해 OTP를 사용하거나 패스워드 길이를 증가시키고, 특수기호를 포함하는 패스워드를 생성하게 하는 방안들이 적용되고 있다. 그러나 OTP 장치의 구입비용 발생, 복잡한 패스워드로 인한 사용자의 편리성 저하 등 실용성의 문제가 있다. 무엇보다 단방향 인증 기반에서는 여전히 취약점이 존재한다. 이를 해결하기 위해 본 논문에서는 QR-Code를 활용한 다중채널, 다중요소 인증 시스템을 제안한다. 제안하는 시스템은 상호 인증을 제공하여 피싱이나 파밍과 같은 공격에 대응할 수 있다. 또한 휴대용 스마트 기기를 OTP 생성기로 활용하여 사용자의 편리성을 보장하면서 기존 패스워드 공격들에 대응할 수 있다.

Key Words : QR-Code, Mutual Authentication, Smart device

ABSTRACT

Password based authentication systems are most widely used for user convenience in web services. However such authentication systems are known to be vulnerable to various attacks such as password guessing attack, dictionary attack and key logging attack. Besides, many of the web systems just provide user authentication in a one-way fashion such that web clients cannot verify the authenticity of the web server to which they set access and give passwords. Therefore, it is too difficult to protect against DNS spoofing, phishing and pharming attacks. To cope with the security threats, web system adopts several enhanced schemes utilizing one time password (OTP) or long and strong passwords including special characters. However there are still practical issues. Users are required to buy OTP devices and strong passwords are less convenient to use. Above all, one-way authentication schemes generate several vulnerabilities. To solve the problems, we propose a multi-channel, multi-factor authentication scheme by utilizing QR-Code. The proposed scheme supports both user and server authentications mutually, thereby protecting against attacks such as phishing and pharming attacks. Also, the proposed scheme makes use of a portable smart device as a OTP generator so that the system is convenient and secure against traditional password attacks.

※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2014-H0301-14-1010)
◆ First Author : Department of Information and Communication, Duksung women's university, jiyepark@duksung.ac.kr, 학생회원
° Corresponding Author :Departtment of Digital media, Duksung women's university , kang@duksung.ac.kr, 정회원
* 덕성여자대학교 네트워크 보안 연구실 sny14@naver.com, minssu17@gmail.com
논문번호 : KICS2013-11-504, Received November 23, 2013; Revised January 21, 2014; Accepted April 11, 2014

Ⅰ. 서 론

하드웨어의 집적 기술과 통신 기술의 발달로 개인당 소유하고 있는 스마트 기기 수는 기하급수적으로 증가하고 있다. 이러한 환경의 변화로 과거 컴퓨터 중심의 웹 서비스들이 스마트 폰이나 스마트 TV와 같은 다양한 스마트 기기에서 이용되고 있다[1].

다양한 스마트 기기와 다양한 플랫폼에서 동작되는 웹 기술의 발전은 사용자들에게 언제 어디서나 웹을 이용할 수 있게 하는 기틀을 마련해 주었다. 하지만 웹 서비스 제공자는 수많은 종류의 스마트 기기와 웹 브라우저에 적합한 이종 플랫폼을 각각 제공해야 하는 부담이 증가하게 되었다. 사용자 또한 기기에 따라 이종의 플랫폼을 설치해야 하고 사용하는 스마트 기기의 증가 로 인해 인증 시 보안 정보의 유지 및 관리가 어려운 문제가 발생된다.

패스워드 기반 인증 시스템은 현재 웹 사이트에서 가장 많이 사용하고 있는 인증 시스템이다. 높은 사용률에도 불구하고 패스워드는 이미 오래전부터 제로데이 공격, 패스워드 추측공격, 사전식 대입공격, 키 로깅 공격 등 다양한 공격에 취약하다. 사용자들은 '12345' 나 'password'와 같은 추측하기 쉬운 패스워드를 사용할 뿐만 아니라 비밀번호를 주기적으로 변경하지 않아 계정정보 유출의 위험에 노출되어 있다[2]. 이 밖에도 편의를 위해 여러 웹 사이트에 동일한 비밀번호를 사용하다보니 보안이 취약한 웹 사이트의 계정이 유출되었을 경우 같은 정보를 사용하는 모든 웹 사이트가 침해되는 2차 피해가 발생한다.

계정정보 유출의 위험을 줄이기 위해 많은 웹 서비스 제공자들은 패스워드 길이를 증가시키고, 특수기호를 반드시 입력하게 하는 등 노력을 기울이고 있다. 하지만 사용자의 동일한 패스워드 사용으로 인해 발생되는 2차 피해에는 여전히 대응할 수 없다. 또한 복잡한 패스워드를 기억하기 힘들어하는 사용자들이 문서나 메일에 계정정보를 기록하다보니 또 다른 보안의 취약성이 되기도 한다.

상기 기술한 패스워드 노출 위험 이외에 인증 처리 범위와 주체도 문제가 될 수 있다. 대부분의 패스워드 기반 인증 시스템은 웹 서버가 사용자를 인증하는 단방향 인증만을 제공하고 있다. 단방향 인증의 경우 사용자는 아이디와 패스워드의 입력 시 해당 사이트가 적합한 웹 사이트인지 검증 할 수 없다. 웹 서비스의 보안은 사용자 측면과 더불어 서버에서 제공하는 보안 기능도 매우 중요하다. 이를 위해 국내의 경우 2012년 8월 정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정으로 SSL(Secure Socket Layer)/TLS(Transport Layer Security) 기술[3,4] 적용이 필수가 되었다. SSL/TLS는 상호 인증, 기밀성 보호, 무결성 보호 등을 제공하는 전송계층 보안 기술이다. 그러나 웹 서버의 성능 저하를 피하거나 운영비용의 절감을 이유로 법령을 준수하는 수준에서 제공하는 보안 서비스는 여전히 취약하다. 또한 웹 서비스에 SSL을 적용하더라도 DNS공격, ARP 공격, 세션우회 공격 등으로 피싱이나 파밍 사이트로 사용자를 유도할 수 있다. 피싱/파밍 공격에 대응하기 위해 금융권 등에서 사이트키(SiteKey) 방식을 사용하기도 하지만 여전히 다양한 보안 위협이 존재 한다[5].

이러한 문제점들을 해결하고자 인증 시 사용자가 가지고 있고(What you have), 자신만 알고 있으며(What you know), 사용자 자신의 정보(What you are)를 복합하여 활용하는 다중 요소(Multi-Factor) 인증[6], 다중 채널(Multi-Channel) 인증[7] 기술들이 제안되고 있다. 그리고 1회용 패스워드(즉, OTP: One Time Password)를 인증에 이용하여 패스워드가 가진 한계점을 해결하고자 하였다[8]. 하지만 사용자가 OTP 발생 장치를 항상 소지해야 하는 조건, OTP 장치의 구입비용 발생, 각각의 웹 서비스를 이용하기위해 각 웹서비스 마다 등록해야 하는 불편함은 패스워드를 이용한 현 인증 시스템을 대신하는데 많은 제약이 되고 있다.

상기 제시한 취약성을 해결하기 위해 본 논문에서는 스마트 기기와 QR-Code를 활용한 두 가지 채널(Two-Channel), 두 가지 요소(Two-Factor) 인증 시스템을 제안한다. 특히, 제안하는 시스템은 서버와 사용자 간 상호 인증을 제공하므로 피싱, 파밍과 같은 공격에 대응할 수 있다. 사용자의 인증에는 OTP를 적용하여 패스워드의 다양한 취약성을 보상한다. 서버 인증의 경우에는 사이트키의 방식과 유사하지만 접속 시 마다 변경되는 검증 값을 사용한다.

본 논문은 다음과 같이 구성된다. 2장에서는 웹 서비스 인증을 위해 제안된 관련 기술에 대하여 살펴보고, 3장에서는 제안 시스템의 동작 모델을 기술한다. 4장에서는 제안 시스템 구현 결과를 바탕으로 동작시험 및 보안 분석에 대해 기술한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

높은 사용률에도 불구하고 패스워드 기반 인증 방식은 이미 오래전부터 패스워드 추측공격이나 사전식

대입 공격 등 다양한 공격에 취약한 것으로 알려져 왔다. 또한 사용자와 서버를 상호 인증하지 않아 피싱이나 파밍 공격 사례들이 많이 보고되고 있다. 이를 해결하기 위해 SSL/TLS 기술과 사이트키 방식 등이 사용된다. SSL/TLS는 다양한 옵션으로 서버와 사용자가 상호 인증된다. 인증 후 연결이 개시되면 암호화와 MAC을 이용하여 데이터 기밀성과 무결성이 제공된다. 그러나 그림 1에 표시한 것처럼 시스템의 hosts 파일을 단순히 변경하거나 바이러스, 트로이웜 등을 이용해 거짓 사이트로 유도하는 공격에는 대응하기 어렵다.

금융권 등의 웹 서비스에서는 이러한 거짓 사이트 유도에 대응하기 위한 방안으로 사이트키 방식을 적용하고 있다. 그러나 등록 시 설정한 이미지나 텍스트의 경우 일정 시간 후 기억이 용이하지 않고 고정된 이미지는 중간자 공격에 취약하다[9].

상기 기술한 다양한 공격과 패스워드 기반 인증 시스템의 취약점에 대응하기 위해 다채널, 다요소 인증 기술들이 제안되고 있다. QR-Code는 패스워드와 함께 두 가지 인증 요소로 많이 활용된다. QR-Code를 촬영하는 스마트 기기의 이용으로 두 가지 채널 인증을 동시에 제공함으로 보다 안전한 인증 서비스를 제공할 수 있다[7,11-13].

스마트 기기를 활용한 두 가지 채널로 클라이언트가 서버를 인증 할 수 있는 시스템을 제안한[7]의 경우, 서버 인증을 위해 클라이언트의 ID값, 서버의 키 값을 해시하여 랜덤 넌스 값과 XOR 연산하여 타임스탬프와 함께 전송한다. 하지만 타임스탬프 값이 암호화 되지 않고 전송되므로 공격자가 타임스탬프 값을 조작할 경우, 중간자 공격에 대응 할 수 없다. 또한 서버의 키 값과 사용자의 ID값을 해시한 값은 변하지 않으므로 랜덤 넌스 값이 쉽게 노출 되는 등의 보안문제가 존재한다.

Challenge-Response 인증 기반인 Snap2Pass 시스템[10]은 웹에서 패스워드기반 인증 시스템을 이용했을 경우 발생할 수 있는 보안 문제점들에 대응할 수 있는 인증 시스템이다(그림 2 참조).

Snap2Pass는 CRYPTOCard나 RSA을 이용한 인증 시 소요되는 시간을 크게 단축하였다. Snap2Pass 시스템에서는, 사용자 계정 생성 시 제공되는 128bit의 키를 스마트 폰에 저장하며 추후 웹 서버와 사용자간 challenge-Response를 통한 인증에 사용된다. 하지만 128bit의 키는 서버에서 설정된 값이므로 사용자가 기억하기에 용이하지 않다. 따라서 키가 저장되어 있는 스마트폰을 분실 할 경우, ID와 패스워드를 이용한 키 변경에 어려움이 있다. 또한 계정 생성 시 계정정보를 담은 QR-Code를 암호화 없이 그대로 제공하므로 중간자 공격에 계정정보가 그대로 노출 될 위험이 있다.

중간자 공격에 대응 할 수 있는 인증 방법으로 서명을 이용한 QR-Code 인증 기법이 있다[11]. 제안 방식에서는 중간자 공격 대응 및 서버와 사용자의 상호 인증을 위해 서버의 개인키로 서명이 된 QR-Code를 이용하여 인증을 진행한다. 하지만 사용자는 서명 인증을 위해 별도의 어플리케이션으로 서버의 인증서를 다운받아야 하는 불편함이 있다. 여러 웹 사이트에서 제안 시스템을 사용할 경우, 각각 웹 사이트 인증서를 휴대폰에 모두 소지해야 하고 관리해야 하므로 실용성이 저하된다.

이 밖에 사용자 인증에 사용되는 OTP 값의 유출을 방지하기 위한 방법으로 QR-Code를 활용한 인증 시스템이 제안되었다[12]. 하지만 사용자의 PC가 악성코드에 감염이 되어있을 경우 OTP값 유출에 대응하기 위한 제안 시스템임에도 불구하고 서버 인증을 위해 사용자의 계정과 비밀번호를 PC에 입력하여 서버 인

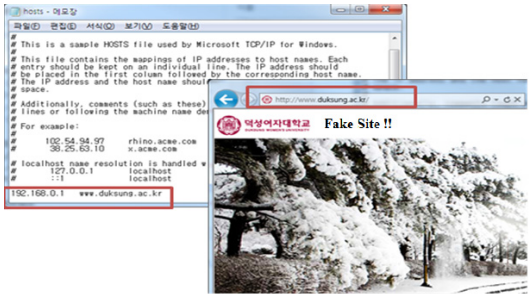


그림 1. hosts 파일 변조를 통한 접속 유도 공격
Fig. 1. Redirect attack by modifying the hosts file

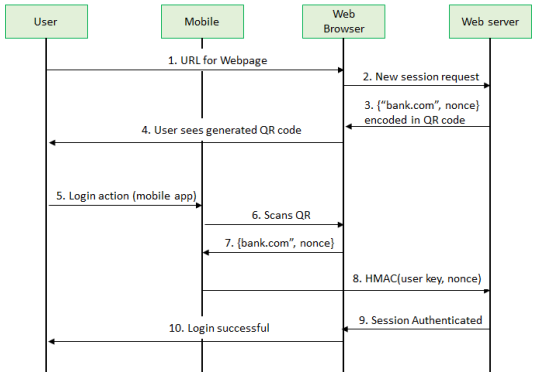


그림 2. Snap2Pass의 인증시스템 동작과정
Fig. 2. A sequence diagram for System of Snap2Pass

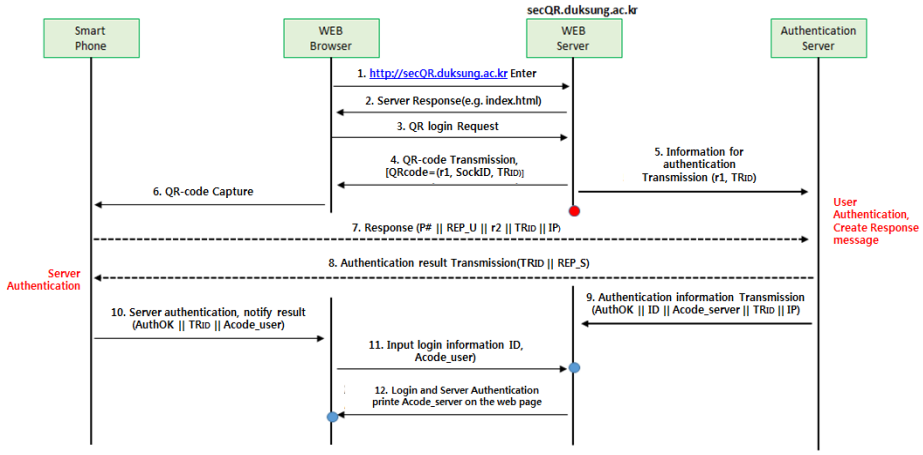


그림 3. QR-Code 인증 시스템 동작 과정
Fig. 3. Proposed system flow about QR-Code authentication

증을 수행해야 한다. 따라서 사용자 PC가 감염되었을 경우 계정 정보가 유출 되는 한계점이 남아있다.

Ⅲ. 제안 시스템

본 장에서는 웹 서비스 이용 시, QR-Code와 스마트 기기를 이용한 두 가지 요소, 두 가지 채널 인증을 통해 사용자와 서버가 상호 인증할 수 있는 인증 시스템을 제안한다.

다음 표 1은 본 논문의 제안 시스템에서 사용하는 파라미터들을 나타낸다.

본 논문의 가정 사항은 다음과 같다.

- 인증 시 사용되는 스마트 기기는 악성코드나 바이러스에 감염되지 않은 안전한 기기이다.
- 개인 정보유출로 인한 2차 피해에 대응하기 위해 서비스 사용자의 스마트 폰에는 사용자가 지정한 보안 등급에 따라 패스워드가 안전하게 되어 저장되어 있다.
  높은 보안을 요구하는 웹 사이트의 경우 각 사이트 별로 해시 된 패스워드가 저장된다.
- 인증 서버의 데이터베이스에는 사용자의 ID와 해시된 패스워드, 사용자의 핸드폰 번호가 안전하게 저장되어있다.
- 웹 서버와 인증 서버는 백 엔드(Back-end) 서비스로 서비스 제공자의 보안 정책에 따라 안전한 보안 프로토콜이 제공되고 있다.

표 1. 시스템 파라미터
Table 1. System Parameter

Parameter	Context
r_1,r_2	Random nonce (128bit)
$Sock_{id}$	IP, Port number of authentication server
TR_{id}	Transaction Identifier
$P\#$	Phone number
$H(pw)$	Hashed Password
OTP	One time Password
$ACode\_user$	Login Password
$ACode\_server$	Authentication Code

동작 과정은 다음과 같다 (그림 3. 참조).

1) 서비스 페이지 최초 접속 요청

웹 서비스 사용자는 웹 브라우저에 URL을 입력하여 해당 서버에 초기 페이지 전송을 요청한다.

2) 웹 서버 응답

웹 서버는 서비스 사용자에게 해당 서비스의 초기 페이지를 전송한다. 상기 과정은 일반 웹 클라이언트와 서버의 요청, 응답 과정과 동일하다.

3) QR-Code 로그인 요청

서비스 사용자는 웹 서버에 QR-Code를 이용한 사용자, 서버 간 상호 인증 로그인 서비스 개시를 요청한다.

4) QR-Code 전송

웹 서버는 128bit의 랜덤 넌스 값 r_1, 인증 서버의 IP 주소와 Port 번호 정보에 해당하는 $Sock_{id}$, 트랜잭션을 구분하기 위한 TR_{id}를 수식 (1)과 같이

QR-Code로 인코딩하여 로그인 페이지와 함께 웹 브라우저에 전송한다. TR_{id}는 상태를 유지하지 않는 웹 서비스의 특성을 감안하여 향 후 동일한 트랙젝션을 구분하기 위해 사용된다. 웹 브라우저는 QR-Code와 함께 자바스크립트를 이용하여 사용자의 IP 주소 정보를 출력한다. 사용자의 IP 주소 정보는 차후 중간자 공격 대응에 사용된다.

$$QR-Code = Encode(r_1, Sock_{id}, TR_{id}) \quad (1)$$

본 논문에서는 설명의 편의를 위해 1) 과정부터 4) 의 과정을 나누어 설명하였지만 인증 트랜잭션 감소와 사용자의 편의를 위해 2)번 과정에 QR-Code가 함께 전송 될 수 있다 (즉, 3, 4과정 포함).

5) 인증 서버에 정보 전달

웹 서버는 웹 브라우저에 전송한 r_1과 TR_{id} 정보를 인증 서버에 전송한다. 전송된 정보는 사용자가 QR-Code 촬영 시 스마트 폰에서 인증서버로 전송되는 인증 값을 검증하는데 사용된다.

6) QR-Code 스캔

사용자는 본인의 스마트 폰을 이용하여 웹 브라우저에 출력된 QR-Code를 촬영한다.

7) QR-Code 디코딩 및 응답

웹 브라우저에 출력된 IP 주소 정보를 입력한 후, QR-Code를 촬영한다. 스마트 폰은 디코딩을 통해 얻어진 r_1과 사전에 안전하게 저장된 사용자의 패스워드 $H(pw)$를 HMAC의 메시지 값과 키 값으로 각각 사용한다. HMAC의 결과 값으로 얻어진 REP_U는 인증서버에서 사용자를 인증하는 값으로 사용 한다 (수식 (2)). 이후 서버를 인증하기 위해 128 bit 랜덤 넌스 r_2를 생성한 후, 사용자의 휴대폰 번호 $P\#$, REP_U, r_2와 트랜잭션 아이디 TR_{id}, 입력된 IP 주소 정보를 병합하여 인증서버에 전송 한다 (수식(3)).

$$REP\_U = HMAC(H(pw), r_1) \quad (2)$$

$$REP_{msg} = P\# \| REP\_U \| r_2 \| TR_{id} \| IP \quad (3)$$

8) 사용자 인증 및 응답

인증 서버는 웹 서버로부터 전송받은 TR_{id}와 사용자의 스마트 폰으로부터 전송받은 TR_{id}를 비교한 후, $P\#$를 이용하여 사용자의 아이디와 패스워드 $H(pw)$를 검색한다. 웹 서버로부터 전달받은 r_1과 $H(pw)$를 이용해 REP_U을 검증하고 동일한 값이 계산 될 경우 올바른 사용자로 인증한다. 인증 후, 전송받은 r_2과 해시된 패스워드를 이용하여 수식 (4)에 나타낸 암호학적 해시 결과와 TR_{id}를 사용자의 핸드폰에 전송한다.

$$REP\_S = HMAC(H(pw), r_2) \quad (4)$$

9) 인증 정보 웹 서버에 전달

인증 서버는 사용자의 스마트 폰으로 REP_S 메시지 전송 후, 수식 (5)와 같이 OTP로 사용할 패스워드를 생성한다. 그 후, 웹 서버로 인증 완료 알림 메시지와 함께 사용자의 ID, OTP, TR_{id}, 사용자의 IP 주소 정보를 웹 서버에 전송한다.

$$OTP = HMAC(H(pw), r_1 \oplus r_2) \quad (5)$$

10) 인증 서버 인증 및 인증 결과 알림

사용자의 스마트 폰은 TR_{id}를 이용하여 전송했던 r_2를 검색 한 후, REP_S를 검증한다. 만약 적합한 인증 서버임이 확인된 경우 수식 (5)를 이용하여 OTP를 생성한다. 이를 통해 사용자도 서버를 인증함으로써 파밍, 스미싱과 같은 공격에 대응 할 수 있다.

11) 사용자 로그인 정보 입력

최종 로그인 단계에서 사용자는 웹 브라우저에 자신의 아이디를 입력한 후, 스마트 폰 화면에 출력된 OTP 정보 중 앞 5자리에 해당하는 $ACode_user$를 패스워드로 입력한다. $ACode\_user$ 사용을 통해 패스워드 길이를 조절할 수 있어 사용자들의 편리성과 일회용 패스워드의 장점을 모두 포함 할 수 있다. $ACode_user$는 숫자와 대소문자를 구분하는 알파벳으로 구성되므로 62의 5승, 약 9만 1천분의 1의 엔트로피를 가진다. 이는 사용자가 한번 로그인 하는 동안 사용하기에 충분히 안전하다.

12) 로그인 완료 및 웹 서버 인증

웹 서버는 9) 과정에서 전달받은 메시지를 이용하여 사용자의 IP 주소 정보, 아이디와 패스워드 $ACode_user$를 검증한 후 인증 완료 페이지를 출력한다. 이 때, 인증서버로부터 정확한 데이터를 전달

받은 웹 서버임을 증명하기 위해 OTP의 뒤 5자리를 $ACode_server$로 사용하여 페이지 상단에 사용자의 이름과 함께 출력한다. 이 값이 접속 시 마다 변경되는 사이트키의 역할을 수행하게 된다. 만약 사용자의 IP 주소와 9) 과정에서 전송받은 IP 주소 정보가 일치하지 않는다면, 중간자 공격으로 간주하고 인증과정을 종료한다.

본 논문에서 제안하는 시스템의 경우, 일반적으로 사용하고 있는 OTP 발생기기를 이용한 인증 방법과 비교할 수 있다. 본 제안 시스템은 사용자가 휴대하고 있는 스마트 기기를 이용하므로 OTP 발생기기 구입을 위한 추가 구입비용이 발생하지 않는다. 또한 단일 기기로 다양한 웹 서비스에 적용할 수 있으므로 서비스 단위로 사용해야하는 OTP의 부담을 완화할 수 있다. 또한 사용자와 서버가 공유한 랜덤 넌스를 사용하여 사용자와 서버가 함께 패스워드를 생성 할 수 있다는 장점이 유도 된다.

Ⅳ. 동작 시험 및 보안 분석

4.1 동작 시험

본 절에서는 제안한 시스템을 구현하여 시험 한 결과를 기술한다. QR-Code를 이용한 인증 요청 시 전송받은 화면은 다음 그림 4와 같다.

그림 4는 웹 서버로부터 전송받은 128bit의 랜덤 넌스 값 r_1과 인증 서버의 IP 주소와 Port 번호 정보에 해당하는 $Sock_{id}$ 정보, 트랜잭션을 구분하기 위한 TR_{id}를 포함한 QR-Code를 포함하고 있다.

사용자는 그림 4의 QR-Code 정보를 스마트 폰으로 촬영하여 서버와 사용자간 상호 인증을 수행한다. 인증에 성공하였을 경우, 사용자의 스마트 폰에는 위

그림 4. QR-Code 로그인 화면
Fig 4. QR-Code login screen

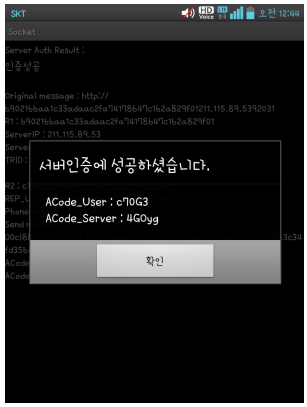


그림 5. 스마트폰 인증 성공 메시지
Fig. 5. Authentication success message

그림 5와 같은 결과 화면이 출력된다. 128bit 랜덤 넌스와 해시된 패스워드를 이용해 생성한 일회용 패스워드 중 앞 5글자를 사용자가 입력하는 패스워드로 사용한다. 또한 뒤 5글자는 서버를 인증하는 사이트키 검증값으로 사용된다.

그림 4의 ID, OTP 입력란에 정보를 입력한 후, 인증이 성공했을 경우 위 그림 6과 같이 사용자의 이름과 웹 서버 인증 값(사이트키 값)이 브라우저에 출력된다. 앞에 기술했듯이, 웹 서버 인증 값은 일회용 패스워드의 맨 끝 다섯 자리를 사용하며, 사용자는 모바일 화면에 출력된 $ACode_server$의 값과 비교하여 웹 서버를 검증 할 수 있다.

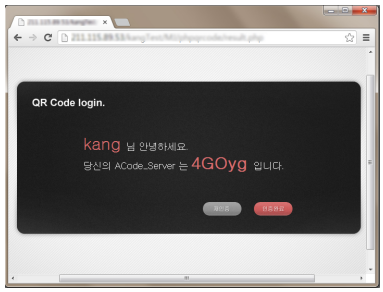


그림 6. 인증 후 웹 페이지
Fig. 6. Web page after authentication

4.2 보안 분석

제안 하는 시스템의 안전성을 분석하기 위해 인증 시 발생할 수 있는 대표적인 공격인 파밍 공격, 재전송 공격, 키 로깅 공격에 대해 분석한다. 표 2는 보안 분석에 사용되어 지는 파라미터들을 나타낸다.

- 파밍공격 (피싱/스미싱 공격 포함)

표 2. 보안 분석 파라미터
Table 2. Security analysis Parameter

Parameter	Context
U	User
U_{mobile}	User's smart phone
S	Server
S_{fake}	Forged Server
A	Attacker
QR_Code	QR-Code
QR_Code_{fake}	Forged QR-Code

사용자 U는 호스트 파일 변조나 악성코드 감염으로 인해 위조된 웹사이트에 접속되어 위조된 QR-Code인 QR_Code_{fake}를 전송받는다.

공격 시나리오
(1) $U \rightarrow S_{fake}$: 위조된 웹 서버 유도 접속
(2) $QR\_Code_{fake} \rightarrow U$: 위조된 QR-Code 출력
대응 방안
(1) QR_Code_{fake} 촬영
(2) $U_{mobile} \rightarrow S$: 위조된 QR-Code 서버 전송 $(P\#, REP\_U, r1_{fake}, TR_{id}, IP)$
(3) $S \rightarrow U_{mobile}$: REP_S 계산 불가

사용자는 공격 사실을 알 수 없으므로 위조된 서버에게 $(P\#, REP_U, r1_{fake}, TR_{id}, IP)$를 전송한다. 그러나 위조된 서버는 암호학적 해시에 사용할 $H(pw)$를 획득할 수 없어 응답 메시지를 생성할 수 없으므로 공격이 불가하다.

• 재전송 공격 (Replay attack)

본 제안 시스템의 인증과정 중, 최종 인증 값 입력 단계에서 인증 값$(ID, ACode_user)$를 웹 브라우저에 직접 입력하여 전송하는 과정에서 공격자가 입력되는 모든 정보를 가지고 있다가 일정시간 이후 인증 값을 재사용하는 재전송 공격을 할 수 있다.

공격 시나리오
(1) $U \rightarrow A$: 공격자가 인증정보 가로챔
(2) $A \rightarrow S$: 일정 시간이 흐른 후, 가로챈 인증 정보로 인증 시도
대응 방안
(1) $S \rightarrow U$: 매 인증시마다 새로운 넌스 전송
(4) $A \rightarrow S$: 기존 인증 정보로 인증 시도
(3) $S \rightarrow A$: 서버의 인증 불가 알림

제안 시스템에서는 매 인증 요청 시 마다 서로 다른 각각의 랜덤 넌스 $(e.g., r_1, r_2 \cdots)$를 사용하여 서로 다른 $ACode_user$를 사용 하므로 패스워드 $ACode_user$는 매번 달라진다. $ACode_user$는 일회성 비밀번호와 같은 의미로 사용 되므로 재전송 공격에 대응 할 수 있다.

• 키로깅 공격 (KeyLoging Attack)

다수가 사용하는 공공시설의 컴퓨터는 KeyLogger 프로그램과 같은 악성 프로그램이 설치될 수 있다.

공격 시나리오
(1) $U \rightarrow S$: 사용자가 서버로 인증 요청
(2) $QR\_Code \rightarrow U$: QR-Code 전송
(3) $U_{mobile} \rightarrow S$: QR-Code 촬영 후 사용자 인증 값 전송
(4) $S \rightarrow U_{mobile}$: 서버 인증 값 전송
(5) U_{mobile} : 인증 완료 알림
(6) $U \rightarrow S$: 로그인 과정에서 A가 로그인 정보 가로챔
대응 방안
(1) $A \rightarrow S$: (6)에서 획득한 정보를 이용하여 로그인 시도
(2) $S \rightarrow A$: (6)에서 획득한 정보는 일회용 패스워드 이므로 인증 불가 알림

이 경우 사용자는 개인 스마트 폰을 이용한 QR-Code 인증을 통해 생성된 일회용 패스워드($ACode\_user$)를 이용하여 웹 서버에 접속 할 수 있다. 따라서 공격자는 아이디와 패스워드를 수집 했다 하더라도 재사용 할 수 없어 KeyLogger 공격에 대응할 수 있다.

• 중간자 공격 (Man-In-The-Middle Attack)

본 제안 시스템에서 사용자의 웹 브라우저와 웹 서버 간 공격자가 존재할 수 있다. 공격자가 웹서버로부터 전송받은 QR-Code 값 $(r1, Sock_{id}, TR_{id})$를 그대로 사용자에게 전달할 경우, 모바일 기기를 이용한 사용자 인증 요청 시 서버에서 사용자 인증이 완료 된다. 따라서 공격자는 사용자가 최종 입력하는 $ACode\_user$ 값을 가로채 웹 서버로부터 올바른 사용자로 인증 받을 수 있다. 이와 같은 중간자 공격에 대응하기위해 QR-Code 촬영 시, 웹 브라우저에 출력되는 IP 주소 정보를 또 다른 인증 채널인 스마트 폰과 인증 서버 간 통신 시 함께 전송 $(P\#, REP_U, r_2, TR_{id}, IP)$한다. 인증 서버는 웹 서버에 IP 주소와 함께 인증 정보를 제공하여 최종 로그

인 과정에서 해당 브라우저의 IP 주소를 검증하여 IP 주소가 일치하지 않거나 두 개의 IP 주소에서 로그인 시도 시 인증과정을 종료한다. 따라서 중간자 공격에 대응 할 수 있다.

공격 시나리오
(1) $A \rightarrow S$: QR-Code 요청
(2) $QR\_Code \rightarrow A$: QR-Code 전송
(3) $U \rightarrow S_{fake}$: 공격자의 서버로 인증 요청
(4) $QR\_Code \rightarrow U$: 공격자가 기존에 갖고 있던 QR-Code 전송
(5) $U_{mobile} \rightarrow S$: 인증 정보 전송
(6) $U \rightarrow S_{fake}$: 인증 시도
(7) $A \rightarrow S$: S_{fake}에서 획득한 정보를 이용하여 진짜 서버에 인증 시도
대응 방안
(1) S : A가 전송한 인증 정보와 IP확인
(2) $S \rightarrow A$: 인증 정보의 IP와 A의 아이피가 일치하지 않음으로 인증 불가 알림

• Key Revocation

스마트 기기를 이용하는 경우 도난의 위협은 존재한다. 그러나 도난 시 사용자가 사실을 직시하는 것이 패스워드를 도용되었을 때 보다 빠르고 용이하다. 해시된 패스워드가 저장되어 있는 스마트 폰을 잃어버린 경우, 사용자는 기존 웹 서비스와 동일하게 QR-Code를 이용하지 않는 아이디 패스워드 기반 인증을 통해 쉽게 패스워드를 변경 할 수 있다. 사용자가 패스워드를 변경한 후에 스마트폰을 가진 공격자라도 더 이상 인증에 성공 할 수 없다.

제안 시스템은 사용자의 기억에 의존하지 않는 패스워드를 적용할 수 있으므로 모든 서비스 단위로 복잡하고 긴 패스워드 사용이 가능하다. 따라서 기존 패스워드 기반 방식에서 문제로 지적되었던 패스워드 노출 시 2차 피해가 발생한다는 취약점에도 대응할 수 있다.

표 3. 인증 방법에 따른 공격여부 비교
Table 3. The comparison of authentication Scheme

	Proposed System	ID/PW	OTP
Phishing	×	○	△
Replay	×	○	△
Keylogger	×	○	×
MITM	×	○	○

× : 공격 불가 ○ : 공격 가능 △ : 조건에 따라 공격 가능

다음 표 3에서는 본 논문의 제안 시스템과 아이디, 패스워드 기반 인증 시스템, 기존 사용되고 있던 OTP를 이용한 인증 시스템을 각 보안 공격에 대해 공격 가능 여부를 비교 하였다.

아이디, 패스워드 기반 인증 공격의 경우, 서버인증을 할 수 없으므로 피싱 공격, 중간자 공격에 노출되어있다. 또한 공격자가 아이디, 패스워드를 획득하여 일정시간 후 다시 로그인하는 재전송 공격이 가능하며, 긴 시간동안 패스워드를 변경하지 않고 사용하는 특성 때문에 키 로깅 공격에 취약하다. 따라서 아이디, 패스워드 기반 인증 시스템은 해당 공격에 모두 대응하지 못하므로 비교 인증 시스템 중 가장 취약하다.

OTP 생성기를 이용한 인증 시스템의 경우, 인증 시 마다 패스워드가 변경 되므로 키 로깅 공격에는 효과적으로 대응 할 수 있다. 하지만 OTP를 이용한 인증 방안 역시 서버인증을 하지 않으므로 중간에 공격자가 OTP를 획득하여 바로 사용하는 실시간성 공격일 경우(에, 메모리공격) 피싱 공격이나 재전송 공격, 중간자 공격에 대응 할 수 없다는 한계점이 있다.

본 논문의 제안 시스템에서 생성하는 패스워드는 OTP 특성을 가지므로 키 로깅 공격에 대응 할 수 있다. 또한 사용자의 OTP 정보만을 의존하는 인증 시스템의 한계를 해결하고자 서버의 인증값(사이트키) 역시 OTP의 개념을 적용했다. 즉, 접속 시 마다 변경되는 서버의 인증 값을 검증하여 서버인증을 진행 하므로 다양한 공격에 대응 할 수 있다.

V. 결 론

본 논문에서는 QR-Code를 이용한 두 가지 요소, 스마트 기기를 이용한 두 가지 채널 인증 시스템을 제안하였다. 본 논문의 제안 시스템에서는 랜덤 넌스를 통해 일회용 패스워드를 생성하여 인증에 활용하였다. 일회용 패스워드 생성에 휴대가 편리한 스마트 기기를 이용하므로 별도의 OTP 생성기를 소지 하지 않아도 되며, OTP 생성기 구입을 위한 추가 비용이 들지 않는다. 사용자와 웹 서버 간 상호 인증으로 피싱/파밍/스미싱, 재전송 공격, 키로깅 공격에 대응 할 수 있다. 또한 스마트 폰을 이용하여 패스워드를 생성하므로 사용자가 복잡한 패스워드를 기억하지 않아도 된다는 장점이 있다.

References

[1] J. Park and N. Kang, "Entity authentication

scheme for secure WEB of things applications," *J. KICS*, vol. 38B, no. 05, pp. 394-400, May 2013.

[2] T.I.A.D.C. (ADC), *Consumer password worst practices*, Inquiry 1-5, 2009, from http://www.imperva.com

[3] A. O. Freier, P. Karlton, and P. C. Kocher, "The SSL protocol: Version 3.0," Netscape Draft302, Nov. 1996.

[4] T. Dierks and E. Rescorla, *The transport layer security (TLS) protocol version 1.2*, IETF Standard RFC 5246, Aug. 2008.

[5] S. E. Shechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators," in *Proc. IEEE Security and Privacy*, pp. 51-65, Berkeley, California, May 2007.

[6] S. Michael, "Replacing username/password with software-only two-factor authentication," Cryptology ePrint Archive, Report 2012/148, 2012.

[7] K. Liao, W. Lee, M. Sung, and T. Lin, "A one-time password scheme with QR-Code based on mobile phone," *INC, IMS and IDC,* pp. 2069-2071, Seoul, Korea, Aug. 2009.

[8] L., Men and U. Blumenthal, "Manageable one-time password for consumer applications," in *Conf. Consumer Electronics (ICCE)*, pp. 1-2, Las Vegas, NV, Jan. 2007.

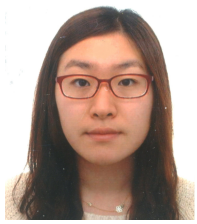
[9] J. Youll, "Fraud vulnerabilities in SiteKey security at bank of america," Review draft to Bank of America/RSA, Jul. 2006.

[10] B. Dodson, D. Sengupta, D. Boneh, and M. Lam, "Secure, consumer-friendly web authentication and payments with a phone," *MobiCASE*, pp. 17-38, Santa Clara, CA, USA, Oct. 2010.

[11] J. Lee, H. You, C. Cho, and M. Jun, "A design secure QR-Login user authentication protocol and assurance methods for the safety of critical data using smart device," *J. KICS*, vol. 37C, no. 10, pp. 949-964, Oct. 2012.

[12] S. Seo, C. Choi, G. Lee, and H. Choi, "QR code based mobile dual transmission OTP system," *J. KICS*, vol. 38B, no. 5, pp. 377-384, May 2013.

박 지 예 (Ji-ye Park)



2013년 2월 : 덕성여자대학교 컴퓨터시스템학과 졸업
2013년 3월~현재 : 덕성여자대학교 전자정보통신학과 석사과정
<관심분야> Internet of Things, 네트워크 보안

김 정 인 (Jung-in Kim)

2011년 3월~현재 : 덕성여자대학교 디지털미디어학과 재학
<관심분야> 네트워크 보안

신 민 수 (Min-su Shin)

2011년 3월~현재 : 덕성여자대학교 디지털미디어학과 재학
<관심분야> 네트워크 보안

강 남 희 (Namhi Kang)

2001년 2월 : 숭실대학교 정보통신대학원 공학석사
2004년 12월 : University of Siegen 컴퓨터공학과 공학박사
2009년 3월~현재 : 덕성여자대학교 디지털미디어학과 조교수
<관심분야> 유무선 인터넷통신, 통신보안, 시스템 보안>