논문 13-38B-05-07

한국통신학회논문지 '13-05 Vol.38B No.05
http://dx.doi.org/10.7840/kics.2013.38B.5.377

QR 코드를 이용한 모바일 이중 전송 OTP 시스템

서 세 현◆, 최 창 열°, 이 구 연*, 최 황 규**

QR Code Based Mobile Dual Transmission OTP System

Se Hyeon Seo◆, Chang Yeol Choi°, Goo Yeon Lee*, Hwang Kyu Choi**

요 약

비밀번호 기반의 사용자 인증은 동일한 비밀번호를 반복 사용하므로 보안이 취약하여 OTP(One-Time Password)가 도입되었다. 하지만 보안이 강화된 OTP를 서버와 동기된 모바일 기기에서 생성하여 PC에 입력하는 경우 PC가 악성코드에 감염되어 있으면 해커가 사용자 계정과 비밀번호 그리고 OTP값을 해킹할 수 있다. 본 논문에서는 OTP값 유출에 따른 보안 취약성을 해소하기 위해 사용자는 계정과 비밀번호를 PC에 입력하여 서버인증을 수행하고, PC 화면에 출력된 QR코드를 모바일 기기에서 스캔하여 OTP값을 직접 서버로 전송함으로써 정보 유출에 따른 해킹을 방지하고 PC에 OTP값을 입력하는 불편함을 줄이는 새로운 이중 인증 방식인 DTOTP를 제안한다. 시스템은 이중 전송을 통해 PC인증 방식의 OTP 보다 향상된 보안성을 제공하면서 기존 OTP 알고리즘을 그대로 사용할 수 있어 구현이 용이하며 은행, 포털 및 게임 서비스 등에 안전하게 활용할 수 있다.

Key Words : Dual Transmission, Mobile Device, QR code, Security, Two-Factor

ABSTRACT

In order to improve the security strength in the password based user authentication, in which the security vulnerability is increased while the same password is repeatedly used, the OTP(One-Time Password) system has been introduced. In the OTP systems, however, the user account information and OTP value may be hacked if the user PC is infected by the malicious codes, because the user types the OTP value, which is generated by the mobile device synchronized with the server, directly onto the user PC. In this paper, we propose a new method, called DTOTP(Dual Transmission OTP), to solve this security problem. The DTOTP system is an improved two-factor authentication method by using the dual transmission, in which the user performs the server authentication by typing the user account and password information onto the PC, and then for the OTP authentication the mobile device scans the QR code displayed on the PC and the OTP value is sent to the server directly. The proposed system provides more improved security strength than that of the existing OTP system, and also can adopt the existing OTP algorithm without any modification. As a result, the proposed system can be safely applied to various security services such like banking, portal, and game services.

Ⅰ. 서 론

비밀번호 기반의 사용자 인증은 동일한 비밀번호를 반복 사용하므로 보안이 취약하여 OTP[1]를 도입하였으며, 최근에는 OTP 토큰이나 카드 대신에 스마트 폰을 OTP(One-Time Password) 기기로 많이

※ 이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2011-0013951)
◆ 주저자 : 강원대학교 컴퓨터정보통신공학전공, x86boa@gmail.com, 학생회원
° 교신저자 : 강원대학교 컴퓨터정보통신공학전공, cychoi@kangwon.ac.kr, 정회원
* 강원대학교 컴퓨터정보통신공학전공, leegyeon@kangwon.ac.kr, 종신회원
** 강원대학교 컴퓨터정보통신공학전공, hkchoi@kangwon.ac.kr, 정회원
논문번호 : KICS2013-01-073, 접수일자 : 2013년 1월 31일, 최종논문접수일자 : 2013년 4월 19일

사용한다[2]. 한편 해킹기술이 발달하면서 사용자는 단순 웹페이지 방문만으로 악성코드에 감염될 수 있고 보안이 취약한 PC방, 카페, 학교와 같은 공공 PC 사용 환경이 늘어나면서 OTP 해킹 사례가 증가하고 있다. 기존 모바일 OTP의 경우, 악성코드가 감염된 사용자 PC에 계정과 비밀번호를 입력하여 1차 서버인증을 수행하면 해커에게도 계정과 비밀번호가 전송되며, OTP 인증을 위한 2차 로그인 시에는 PC에 설치된 악성코드가 서버로 전송되는 OTP 값을 해커에게로 전송하여 사용자의 OTP 인증을 막고 해커가 계정과 비밀번호, OTP값을 사용하여 해킹할 수 있다. 악성코드를 이용한 해커에게 계정정보가 넘어갔을 경우를 대비한 OTP 인증절차가 실제로 필요한 상황에서는 아무 역할을 못한다. 그동안 QR코드를 스캔하여 사용자의 정보를 모바일 기기에 전송하거나 OTP 생성 알고리즘을 변경하여 OTP의 보안성을 강화했다[3-5]. 그러나 기존 연구들은 OTP 자체의 보안성 강화나 바코드와 무선통신으로 모바일 기기에 데이터를 전송하는 방법만을 고려했기 때문에 OTP값 유출에 따른 보안 취약성은 여전히 남아있다.

본 논문에서는 QR코드와 데이터의 전송경로를 이중화하여 OTP값 유출에 따른 보안 취약성을 해소하고 해킹의 위험성을 감소시키는 DTOTP(Dual Transmission OTP) 시스템을 구현하였다. DTOTP는 PC인증 방식과 같이 PC에서 서버로 비밀번호를 전송하지만 OTP값은 모바일 기기에서 직접 서버로 전송하는 인증정보의 분할 경로를 채택하여 해킹의 위험성을 감소시키는 이중 인증 OTP 시스템이다. 사용자는 계정과 비밀번호를 PC에 입력하여 서버인증을 수행하고 PC 화면에 출력된 QR코드를 모바일 기기에서 스캔하여 OTP값을 곧장 서버로 전송함으로써 정보 유출에 따른 해킹을 방지하고 PC에 OTP값을 입력하는 불편함을 해소하는 새로운 이중 인증[6] 방식이다. 해커가 PC를 해킹하더라도 OTP값을 알 수 없고 모바일 기기까지 해킹을 하더라도 모바일 회원번호를 사용해 인증을 하기 때문에 사용자 계정을 유추할 수 없다. 나아가 PC 계정과 모바일 OTP값을 무작위로 맞춰 보더라도 시간에 동기되어 OTP값이 주기적으로 변경되므로 해킹은 어렵다. DTOTP 시스템은 기존의 PC인증 방식의 OTP 알고리즘을 유지하면서 이중 전송을 통해 향상된 보안성을 제공한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 이중인증, OTP, QR코드와 직접 관련되는 요소기술을 비교, 분석한다. Ⅲ장에서는 DTOTP의 시스템 구성, 동작 및 인증과정, 알고리즘을 알아보고 구현한 모바일 애플리케이션의 핵심 기능과 시스템을 적용한 홈페이지를 통해 QR코드의 데이터를 살펴본다. Ⅳ장에서는 본 시스템에 대한 보안성 분석과 TTA에서 제공하는 보안 요구사항을 만족하는지 살펴보고 무작위 대입 공격에 대한 보안성을 분석한다. 마지막으로 Ⅴ장에서 결론과 향후과제를 다룬다.

Ⅱ. 관련연구

2.1. Two-Factor Authentication

2가지 인증으로 안전성을 향상시키는 기법은 something you have, something you know, something you are의 3가지 요소를 가지며 집 열쇠, 비밀번호, 지문 같은 생체 정보가 각각의 예이다[6]. 이들 중 하나만 사용하면 보안성이 취약하므로 서로 다른 2개 요소를 조합하여 이중 인증을 한다. OTP는 사용자가 OTP값을 생성하여 검증하는 인증방식으로서 something you have에 속한다. 모바일 기기에서 QR코드를 스캔하고 OTP를 생성하여 PC에 직접 입력하는 방식[3]에서는 인증정보를 모바일 기기에 전송하는데 QR코드를 사용한다. 또한 모바일 기기에서 생성한 QR코드의 이미지를 전송하고 이를 스캔하여 사용자 인증을 실시하는 방법[4]은 PC가 아닌 모바일 기기에서 사용자 인증을 하기 때문에 OTP값 유출에 따른 보안성 문제는 여전히 남아있다. 본 논문에서는 인증정보를 모바일 기기에 전송하고 모바일 기기에서 생성된 OTP값을 직접 서버로 전송하는데 QR코드를 사용함으로써 악성코드에 따른 정보 유출을 막고 사용자가 OTP값을 입력하는 불편함을 해소한다.

2.2. OTP(One-Time Password)

동일한 패스워드를 반복 사용함에 따른 보안 취약점을 해소하기 위해 난수를 일회용 패스워드로 이용하는 OTP는 서버와의 동기화 여부에 따라 비동기방식과 동기방식으로 분류한다. 비동기방식은 질의응답방식으로서 인증서버로부터 받은 질의 값을 OTP 토큰에 직접 입력하여 OTP를 생성한다. 동기방식에는 시간동기방식과 이벤트방식이 있는데, 각각은 정해진 시간과 인증 서버와 동기화된 횟수를 기준으로 사용자가 인증을 요청할 때마다 OTP값을 생성한다. 1차 OTP를 생성하고 사용자 패스워드를 결합하여 인증서버에 전송[5]하면 OTP 알고리즘의

보안은 강화되지만 OTP를 직접 PC에 입력하는 과정이 필요하고 악성코드에 따른 OTP값 유출이 있을 수 있다. 본 논문에서는 이중경로를 사용하여 데이터를 전송하므로 기존 OTP와는 다른 새로운 something you have에 해당하는 인증 방법을 보인다.

2.3. QR코드(Quick Response Code)

1994년 일본 덴소 웨이브가 개발한 매트릭스형 2D 코드로서 2000년 6월에 ISO/IEC 18004 표준으로 되었다[7]. 기존 OTP는 모바일 기기 화면에 출력되는 OTP값을 사용자가 직접 PC에 입력하기 때문에 PC가 악성코드에 감염되면 사용자 계정과 비밀번호 그리고 OTP값까지 해커에게 전송될 수 있다. 본 논문에서는 OTP값 유출에 따른 해킹을 방지하기 위해 QR코드를 고정된 이미지[8,9]로 사용하는 것이 아니라 사용자 데이터와 로그인 시간을 이용하여 동적[10]로 PC 화면에 출력한다. 모바일 기기에서는 스캔을 통해 출력된 QR코드의 데이터를 전달받아 OTP값을 생성하여 서버에 직접 전송함으로써 보안성을 강화하고 사용자가 OTP값을 입력하는 불편함을 해소한다[11].

Ⅲ. 설계 및 구현

3.1. 시스템 구성

DTOTP 시스템은 그림 1과 같이 사용자 PC와 모바일 기기, 웹 서버와 OTP 인증기관으로 구성된다. 사용자는 PC에서 계정과 비밀번호를 이용하여 서버에 로그인 하면 OTP 로그인을 위한 QR코드가 PC화면에 출력되며 모바일 기기로 QR코드를 스캔한다. 모바일 기기에서는 스캔한 QR코드를 디코딩하고 SEED 알고리즘으로 복호화하여 OTP가입 코드일 경우에는 Member Number(MN)와 Random Number(RN)를 모바일 기기에 저장하고, 인증기관에도 계정과 RN, MN를 저장한다. OTP인증 코드이면 MN과 RN, 그리고 Server Time(ST)을 이용하여 생성된 OTP값을 서버에 전송한다. 서버는 계정과 비밀번호를 이용하여 로그인을 처리한 후 인증기관으로부터 MN를 전송받아 QR코드를 생성하여 사용자 PC에 출력하고, OTP 인증을 확인한 후 로그인을 승인한다. 인증기관은 서버의 요청에 따라 MN을 전송하며 서버가 OTP 인증을 요청하면 OTP를 생성하여 전송받은 OTP와 비교한 후 인증결과를 서버에 다시 전송한다. 표 1에 본 논문에서 사용하는 기호를 설명한다.

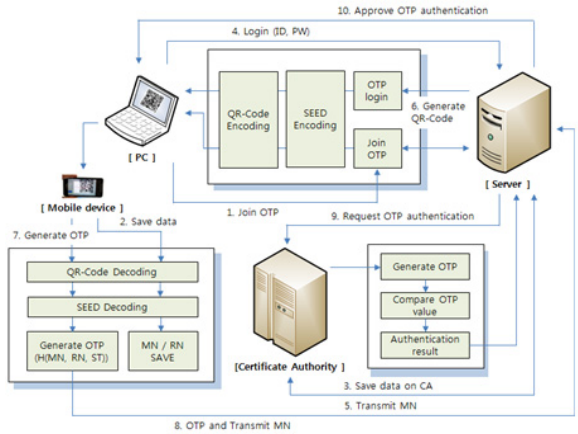

그림 1. DTOTP 시스템의 구성
Fig. 1. Configuration of DTOTP system

표 1. 약어목록
Table 1. List of Acronyms

List of Acronyms	
MN	OTP creation parameter for user identification and cryptographic complexity increase (Member Number)
RN	OTP creation parameter for cryptographic complexity increase (Random Number)
ST	OTP creation parameter for Sync user with server time (Server Time)
AN	Browser session ID for PC identification Session ID (Authentication Number)

3.2. 동작 및 인증과정

DTOTP 시스템의 작업흐름은 그림 2와 같으며 다음 사항을 가정한다. 인증서버는 물리적 공격이나 해킹 등의 보안상 위협으로부터 안전하며, 사용자는 자신의 모바일 기기로 QR코드를 스캔하고 스캔한 QR코드의 디코딩이 가능하다. 사용자는 인증기관 또는 서버가 제공하는 모바일 OTP 생성 알고리즘을 다운받아 이용하며 이 알고리즘은 시간동기방식[12]을 사용한다.

1) PC에서 1차 비밀번호인 계정과 비밀번호를 입력하고 로그인 한다.
2) 서버는 인증기관으로부터 사용자의 MN값을 받아 Authentication Number(AN)와 ST를 SEED 알고리즘으로 암호화하여 QR코드로 변환(QR-Code = EK(MN, AN, ST)), 사용자에게 전송한다.

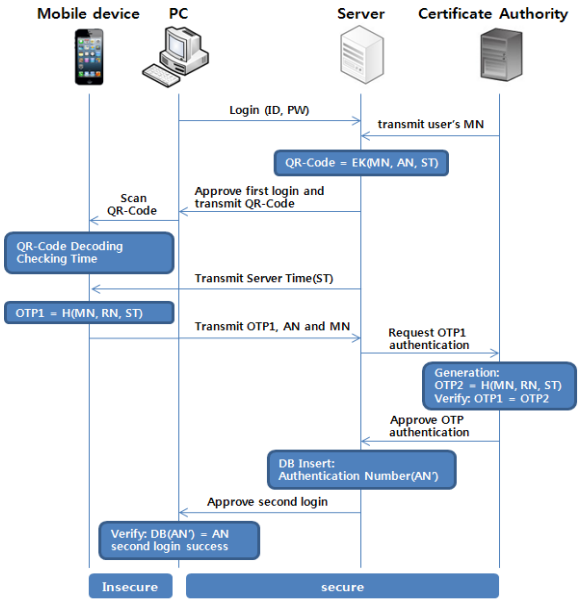

그림 2. DTOTP 시스템의 작업흐름
Fig. 2. Workflows of DTOTP system

3) 사용자 PC화면에 나타난 QR코드를 모바일 기기로 인식하여 디코딩하고 SEED 알고리즘으로 복호화한 다음 ST를 확인해 최신의 QR 코드인지 확인한다. 이때 SEED 알고리즘은 대칭키로 되어있으며 모바일 기기와 서버간의 키 교환을 위해 Diffie-Hellman 방식을 사용한다. 모바일 기기에서는 디코딩된 MN과 OTP 가입 시 모바일 기기에 저장된 MN이 일치하는지 확인하고 MN과 RN, 그리고 서버에서 새로 전송받은 ST를 이용하여 OTP1(OTP1=H(MN, RN, ST))을 생성한다.
4) 생성된 OTP1과 AN, 사용자 확인을 위한 MN을 서버로 전송한다.
5) 서버는 이 데이터들을 확인한 후 인증기관에 OTP1, MN, ST를 전송하고 인증기관에서는 OTP2(OTP2 = H(MN, RN, ST))를 생성하여 전송받은 OTP1과 일치하는지 확인하고 인증 승인 메시지를 서버에 전송한다.
6) OTP 인증이 완료되면 서버는 전송받은 AN을 사용자 데이터베이스에 저장하고 2차 로그인 승인 메시지를 보낸다.
7) PC가 2차 로그인 승인 메시지를 받으면 데이터베이스의 AN과 PC의 AN인 session ID가 일치하는 지를 확인하여 로그인을 수행한다.

3.3. DTOTP 알고리즘

DTOTP를 생성하기 위해 최초 OTP 가입 시 웹 서버로부터 회원번호 12자리와 랜덤번호 6자리를 발급받고 SHA-256 해시 함수를 이용해 해시 값을 생성한다. OTP를 실행할 때 현재시간으로 만든 해시 값과 OTP 가입 시 생성한 해시 값을 XOR 연산으로 256비트의 결과 값을 생성한다. 그 후 추출함수를 이용하여 얻은 결과 값의 특정 비트만을 추출하여 32비트의 OTP 추출 값을 생성한다.

추출함수는 256비트를 32비트씩 8블록으로 나누어 32비트 블록화를 수행한다. 첫 번째 32비트 블록 데이터를 4비트씩 8블록으로 나누어 4비트 블록화를 수행하고 마지막 4비트 블록 값을 7로 나눈 나머지를 선택 값으로 한다. 선택 값으로 남은 7개의 블록 중 하나를 선택해 하나의 4비트 블록을 추출한다. 다른 32비트 블록 또한 같은 방법으로 4비트 블록을 추출하여 32비트의 8자리 OTP값을 생성한다[12].

3.4. 구현

3.4.1. DTOTP 애플리케이션

DTOTP 인증을 위한 QR코드의 출력화면은 그림 3과 같다. 그림 3은 SEED 알고리즘을 적용하기 전의 데이터를 QR코드로 출력시킨 것으로 SEED 암호화를 수행하면 그림 5의 QR코드가 출력된다. 3251-KDFK-1547은 모바일 기기에서 OTP 생성과 사용자 구분을 위해 사용하는 MN으로서 최초 회원가입을 수행하면 랜덤하게 구성된다. &는 데이터를 구분하는 토큰 값이다. 현재의 session ID인 8CDFBFA5B8E7317C74E25A74551B08B2는 로그인 한 PC 사용자를 확인하는 AN이다. 마지막 2012091023331은 년월일시분초로서 서버의 현재시간인 ST를 QR코드에 삽입한다. QR코드 데이터 중 MN과 AN만으로는 무분별한 서버 인증을 방지할 수 없으므로 ST를 QR코드에 삽입하여 모바일 기기에서 인증할 때 QR코드의 ST와 OTP를 생성하기 위해 서버에서 새로 전송받은 ST의 차이가 30초 이내인 경우에만 인증을 수행한다. 이로써 무분별한 인증에 따른 서버의 부담을 줄이고 사용자 위조 등의 공격에 대한 위험을 사전에 방지한다. QR코드에 삽입되지는 않지만 OTP 생성 알고리즘의 매개변수로 사용되는 RN은 MN과 동일하게 최초 회원가입 시 랜덤하게 구성된다. 이는 OTP 알고리즘의 복잡성을 증가시키기 위해 각 사용자에게 다르게 부여되는 초기값이다.

이후의 과정은 OTP 시스템 인증절차의 (3)부터

순서대로 진행하도록 구현하였으며 QR코드 스캔 및 서버에 데이터를 전송한 결과는 그림 4와 같다.

그림 3. 암호화 이전의 QR코드 출력 화면
Fig. 3. QR code output screen before encryption

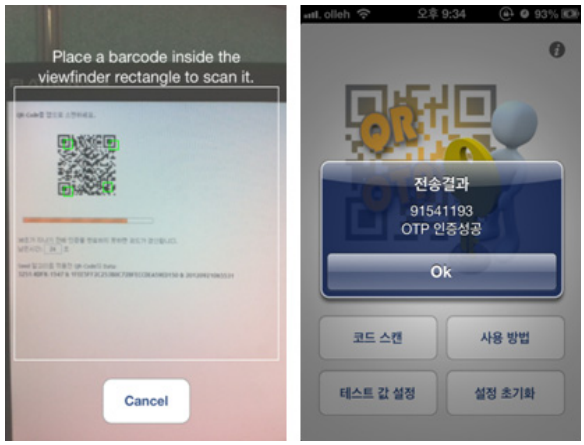

그림 4. QR코드 스캔과 전송결과
Fig. 4. QR code scanning and transmission result

3.4.2. DTOTP 홈페이지

로그인을 하면 그림 5와 같이 SEED 알고리즘이 적용된 QR코드가 출력되며 이 QR코드를 모바일 기기에서 스캔함으로써 로그인이 완료된다.

메인 메뉴에서 코드 스캔 메뉴는 QR코드의 데이터에 따라 자동으로 로그인 코드와 OTP 가입코드를 구분한다. QR코드가 가입이면 데이터가 저장되고 '저장완료'가 출력되며 로그인인 경우에는 인증 상황에 따라 다음 3가지 메시지 중 하나가 출력된다. 계정과 일치하는 MN, RN을 가지고 있는 정당한 사용자가 로그인할 경우에는 그림 4와 같이 OTP 번호와 'OTP 인증성공' 메시지가 출력된다. 데이터베이스에 저장된 MN, RN이 없을 경우 '데이터가 존재하지 않습니다.' 라는 메시지가 출력되고 화면에 출력된 QR코드의 MN과 현재 모바일 기기에 저장된 MN이 다를 경우 '계정과 모바일의 정보가 다릅니다.'를 출력한다. '사용 방법' 메뉴는 애플리케이션을 사용하는 방법을 출력하며, '테스트 값 설정' 메뉴는 OTP 회원가입을 하지 않고 테스트할 수 있도록 admin 계정의 MN, RN을 애플리케이션 데이터베이스에 저장한다. '설정 초기화'는 애플리케이션에 저장된 MN, RN의 데이터베이스를 제거하여 인증 시스템을 초기화하는 메뉴이다.

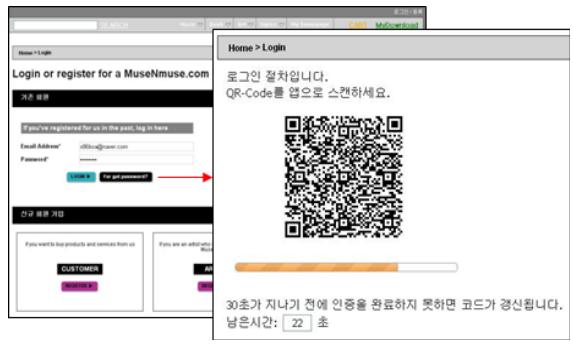

그림 5. DTOTP 시스템 홈페이지
Fig. 5. DTOPT system homepage

은행에서 본인인증을 위해 사용하는 보안카드를 DTOTP 시스템으로 대체할 수 있다. 최초 모바일 애플리케이션에서 공인인증서로 본인인증을 완료하고 서버로부터 사용자 확인을 위한 일련번호와 보안코드 목록을 전송받아 저장한다. 사용자는 PC에 출력되는 QR코드를 스캔하여 일련번호와 QR코드에서 요청한 보안코드 일부를 서버로 전송하며, 서버는 전송받은 일련번호와 보안코드가 일치하는지 확인하여 본인인증을 완료한다. 나아가 포털 및 게임 서비스 등에서도 기존의 OTP 알고리즘을 유지하면서 확장성과 유연성이 우수한 본 시스템을 추가하여 확장할 수 있다.

Ⅳ. 검토 및 분석

4.1. 보안성 분석

Sniffing[4], Password Guessing Attack[13], Replay Attack[13]에 대한 보안성을 분석한다. Sniffing 공격으로 모바일 기기 및 PC의 데이터가 노출되어도 PC와 모바일 사용자가 서로 일치하는지 확인 할 수 없고 PC와 모바일 기기가 서로 다른 경로를 이용하여 데이터를 서버에 전송하기 때문에 안전성이 확보된다. 패스워드를 무작위로 추측하여 대입하는

Password Guessing Attack은 인증 실패 횟수에 따라 공격 유무를 알 수 있으므로 인증 요구 횟수가 많아지면 온라인 패스워드 추측 공격으로 의심하여 인증을 거부할 수 있다. 그리고 본 시스템 같은 시간동기방식에서는 OTP값을 일정 주기로 변경하므로 더욱 안전하다. Replay Attack은 유효 메시지를 골라 복사한 후 재전송하여 정당한 사용자로 가장하는 공격이지만 서버에서 인증할 때 서버의 현재 시간과 QR코드에 사전 삽입된 시간이 30초 이상 차이가 나면 인증을 중단하므로 공격을 방지할 수 있다.

표 2에 DTOTP 시스템과 기존 OTP[14], 이중 인증의 또 다른 방식인 SUAN[14]의 주요 특성을 비교한다.

표 2. 인증 방법의 비교
Table 2. The comparison of authentication methods

	DTOTP	OTP[14]	SUAN[14]
Prevent Typing error	Yes	No	Yes
Two times encryption	Yes	No	No
Communication times each authentication	1	2	6
Encryption algorithm	Hash Function + SEED	Hash Function	Hash function
Two-way authentication	Yes	No	No

4.2. OTP 보안 요구사항 검토

OTP 토큰의 보안 요구 사항[15]을 DTOTP에 적용하고 분석한다. 표준 알고리즘인 SHA-2를 사용하는 OTP 생성은 128비트 이상의 엔트로피를 만족하며 실제로 6자리 이상 9자리 이하 자릿수의 OTP 결과 값을 출력하므로 안전하다. VM 기반 OTP 보안 측면에서는, 서버가 일련번호와 비밀키를 생성할 때 기존에 저장된 데이터베이스와 비교하여 동일한 값이 생성되지 않도록 함으로써 일련번호와 비밀키의 유일성과 무결성을 보장한다. 모바일 OTP에서 토큰을 삭제할 수 있는 인터페이스를 제공하며 OTP를 생성할 때 본인 인증을 함으로써 정당한 사용자임이 확인된다. OTP를 확인하기 전에 전송된 MN값을 먼저 확인하여 정보가 위변조된 경우에는 OTP의 생성을 중지함으로써 부가정보의 가용성과 무결성을 보장한다. 또한 서버에서 전송받은 ST를 사용자가 변경할 수 없으므로 이벤트 정보가 임의로 변경되지 않는 특징이 있다.

4.3. 무작위 대입 공격의 보안성 분석

DTOTP에서는 PC나 모바일 기기 중 어느 하나가 악성코드에 감염되면 해킹은 불가능하며, PC와 모바일 기기 모두가 악성코드에 감염되었을 때는 PC에서 해킹한 계정과 비밀번호로 1차 로그인을 하고 모바일 기기에서 해킹한 OTP값을 무작위로 대입하여 OTP 인증이 성공해야만 해킹이 가능하다. DTOTP 시스템의 사용자가 100명, 500명, 1000명일 때, 무작위 대입 시 일치 확률과 해킹 소요시간을 시뮬레이션 하였다. 이때, OTP값의 갱신주기는 30초, OTP 인증 시 서버의 응답시간은 1000ms이고 기존 OTP는 악성코드에 감염되면 해킹을 당한다고 가정한다.

그림 6은 무작위 대입 공격 시 모바일 기기와 PC가 일치 할 가능성을 보인 것으로 DTOTP 시스템 사용자가 100명일 경우 PC와 모바일 기기의 일치확률은 평균 1%로서 기존 OTP보다 안전하며 사용자 수가 늘어나면 일치 가능성은 더욱 줄어듦을 알 수 있다.

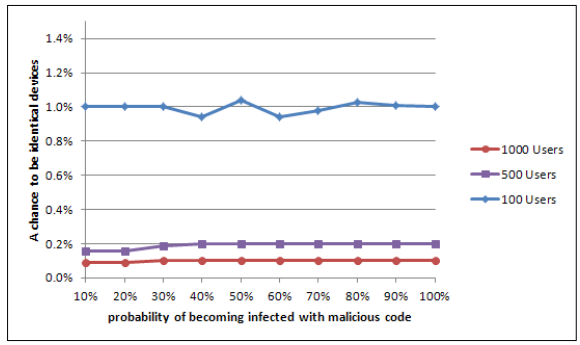

그림 6. 악성코드 감염확률에 따른 기기의 일치 가능성
Fig. 6. A chance to be identical devices by the probability of becoming infected with malicious code

그림 7은 악성코드 감염확률에 따른 해킹 소요시간으로서 사용자가 늘어나면 해킹시간이 증가하여 악성코드 감염확률 보다 시스템의 전체 사용자 수에 더 민감하다. 계정과 OTP값이 일치하는 사용자를 찾더라도 평균 해킹시간보다 OTP 갱신주기가 짧기 때문에 OTP값이 먼저 갱신되어 해킹을 위한 OTP 인증이 실패하게 된다.

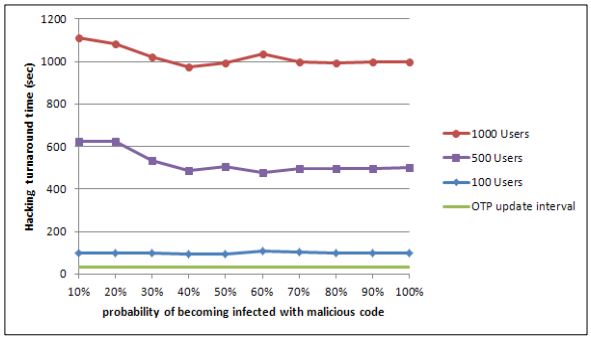

그림 7. 악성코드 감염확률에 따른 해킹 소요시간
Fig. 7. Hacking turnaround time by the probability of becoming infected with malicious code

V. 결 론

비밀번호 기반의 사용자 인증은 동일한 비밀번호를 반복 사용하므로 보안이 취약하여 OTP가 도입되었다. 보안이 강화된 OTP를 서버와 동기된 모바일 기기에서 생성하여 PC에 입력하는 경우 PC가 악성코드에 감염되어 있으면 해커가 사용자 계정과 비밀번호 그리고 OTP값을 해킹할 수 있다.

본 논문에서는 OTP값 유출에 따른 보안 취약성을 해소하기 위해 QR코드와 데이터의 전송경로를 이중화하여 해킹의 위험성을 감소시키는 이중 인증 OTP 시스템을 제안하고 구현하였다. 사용자는 계정과 비밀번호를 PC에 입력하여 서버인증을 수행하고 PC 화면에 출력된 QR코드를 모바일 기기에서 스캔하여 OTP값을 곧장 서버로 전송함으로써 정보 유출에 따른 해킹을 방지하고 PC에 OTP값을 입력하는 불편함을 없앴다. 해커가 PC를 해킹하더라도 OTP값을 알 수 없고 모바일 기기까지 해킹을 하더라도 모바일 회원번호를 사용해 인증하기 때문에 사용자 계정을 유추할 수 없다. 나아가 PC 계정과 모바일 OTP값을 무작위로 맞춰 보더라도 시간에 동기되어 OTP값이 주기적으로 변경되므로 해킹은 어렵다. DTOTP를 위한 모바일 애플리케이션과 홈페이지를 실제로 구현 및 시현하였고, 무작위 대입 공격 상황을 시뮬레이션 하여 기존 OTP에 비해 안전하다는 것을 보였다.

모바일 기기로 데이터를 전송하는 과정을 더 간소화하고 로그인 승인 후 로그인 여부를 주기적으로 체크하는 오버헤드의 감소 방안에 관한 연구는 향후 과제로 남긴다.

References

[1] IETF, *HOTP: An HMAC-Based One-Time Password Algorithm,* RFC 4226, Dec. 2005.

[2] D. H. Shin, Y. S. Choi, S. J. Park, S. J. Kim, and D. H. Won, “Cryptanalysis on the authentication mechanism of the NateOn messenger,” *J. KIISC*, vol. 17, no. 1, pp. 67-80, Feb. 2007.

[3] Y. S. Lee, “Online banking authentication system using Mobile-OTP with QR-code,” in *Proc. 5th Int. Conf. Comput. Sci. Convergence Inform. Technol. (ICCIT)*, pp. 644-648, Dhaka, Bangladesh, Nov. 2010.

[4] S. D. Park, *Mobile authentication system and its application based on 2-dimensional barcode and OTP,* M.S. thesis, Dept. Electron. Comput. Sci. Eng., Graduate School of Hanyang University, Seoul, Korea, Feb. 2009.

[5] J.-H. Che, “A two-factor user authorization method and its implementation using TOTP and password,” *J. KIISC*, vol. 20, no. 6, pp. 7-16, Dec. 2010.

[6] D. DeFigueiredo, “The case for mobile two-factor authentication,” *IEEE Security Privacy*, vol. 9, no. 5, pp. 81-85, Sep. 2011.

[7] AIM, *Uniform Symbology Specification: QR code,* 1996.

[8] Y.-W. Kwon, S.-H. Jung, and C.-B. Sim, “A implementation of gravestone management system based on smart phone using QR-Code,” in *Proc. 2011 Fall Conf. KIECS*, vol. 5, no. 2, pp. 259-263, Gurye, Korea, Nov. 2011.

[9] W. H. Jung and Y. J. Chung, “A design of U-learning study support system using QR code,” in *Proc. 2010 Autumn Conf. KMMS*, vol. 13, no. 2, pp. 607-610, Seoul, Korea, Nov. 2010.

[10] C. H. Ko, S. H. Seo, S. A. Kim, and J. H. Seo, “Smart phone application for intelligent ID management,” in *Proc. 2010 Autumn Conf. KMMS*, vol. 13, no. 2, pp. 641-643, Seoul, Korea, Nov. 2010.

[11] J.-S. Lee, H.-N. You, C.-H. Cho, and M.-S.

Jun, "A design secure QR-login user authentication protocol and assurance methods for the safety of critical data using smart," *J. KICS*, vol. 37, no. 10, pp. 949-964, Oct. 2012.

[12] Y.-S. Jeong, S.-H. Han, and S.-S. Shin, "A study on mobile OTP generation model," *J. Digital Policy Manage.*, vol. 10, no. 2, pp. 183-191, Mar. 2012.

[13] T. I. Song and C. S. Hong, "Energy efficient password-based authenticated group key exchange protocol mechanism using trusted server," *J. KIISE*, vol. 39, no. 4, pp. 350-359, Aug. 2012.

[14] Y.-W. Kao, "Physical access control based on QR code," in *Proc. Int. Conf. Cyber-Enabled Distributed Comput. Knowledge Discovery (CyberC 2011)*, pp. 285-288, Beijing, China, Oct. 2011.

[15] TTA, *Security Requirements for the OTP Token,* Dec. 2010.

서 세 현 (Se Hyeon Seo)

2010년 2월 강원대학교 컴퓨터정보통신공학전공 학사

2013년 2월 강원대학교 컴퓨터정보통신공학전공 석사

<관심분야> 네트워크보안, 모바일컴퓨팅, 데이터베이스시스템, 클라우드컴퓨팅

최 창 열 (Chang Yeol Choi)

1979년 2월 경북대학교 전자공학과 학사

1981년 2월 경북대학교 전자공학과 석사

1995년 2월 서울대학교 컴퓨터공학과 박사

1984년~1996년 ETRI 컴퓨터연구단 책임연구원/연구실장

1996년~현재 강원대학교 IT대학 컴퓨터정보통신공학전공 교수

<관심분야> 컴퓨터아키텍처, 임베디드시스템, 모바일컴퓨팅

이 구 연 (Goo Yeon Lee)

1986년 2월 서울대학교 전자공학과 학사

1988년 2월 KAIST 전기및전자공학과 석사

1993년 2월 KAIST 전기및전자공학과 박사

1993년~1996년 디지콤정보통신 연구소

1996년 삼성전자

1997년~현재 강원대학교 IT대학 컴퓨터정보통신공학전공 교수

<관심분야> 이동통신, 네트워크보안, 인터넷, 초고속통신망, 무선네트워크, 네트워크 성능분석, ad-hoc 네트워크

최 황 규 (Hwang Kyu Choi)

1984년 2월 경북대학교 전자공학과 학사

1986년 2월 KAIST 전기및전자공학과 석사

1989년 8월 KAIST 전기및전자공학과 박사

1990년 3월~현재 강원대학교 IT대학 컴퓨터정보통신공학전공 교수

<관심분야> 데이터베이스시스템, 멀티미디어시스템, 클라우드컴퓨팅