스마트폰의 QR-Code의 인식 기법을 이용한 사용자 인증 기법 설계

이 용 재* · 김 영 곤** · 박 태 성** · 전 문 석***

The Design of User-Authentication technique using QR-Code recognition

Lee, Yong Jae · Kim, Young Gon · Park, Tae Sung · Jun, Moon Seog

〈Abstract〉

Smart phones, greatly expanding in the recent mobile market, are equipped with various features compared to existing feature phones and provide the conveniences to in several ways. The camera, one of the features of a smartphone, creates the digital contents, such photos and videos, and plays a role for the media which transmits information, such as video calls and bar code reader. QR-Code recognition is also one of the camera features. It contains a variety of information in two-dimensional bar code type in matrix format, and makes it possible to obtain the information by using smart phones.

This paper analyzes the method of QR-Code recognition, password method-the existing user-authentication technique, smart card, biometrics and voice recognition and so on and thenn designs a new user-authentication technique.

The proposed user-authentication technique is the technique in which QR-Code, which can be simply granted is read by smart phones and transmitted to a server, for authentication. It has the advantages in view that it will simply the process of authentication and conteract the disadvantages, such as brute force attack, man-inthe-middle attack, and keyboard hacking, which may occur in other authentication techniques

Key Words : QR-Code, Smart Phone, Authentication, Security

Ⅰ. 서론

스마트폰이란 기존의 음성통화 중심의 휴대전화 기능에 통신기능 뿐 아니라 본격적인 네트워크 기능과 개인용 휴대 단말인 PDA(Personal Digital Assistant)가 가진 스케줄 기능, 개인정보 관리 기능 등 다양한 기능을 가진 단말기를 말한다. 차세대 휴대전화라고 불리며, 휴대용 단말기를 통해 음성통화는 물론 화상통화 및 전송, MP3 기능을 통한 음악감상과 DMB로 방송 콘텐츠도 즐길 수 있다. 또한 카메라를 통한 다양한 디지털 컨텐츠를 생성 가능하며, 바코드 리더 등의 기능을 한다. 지난 2009년 4월 관제형 WIPI(Wireless Internet Platform for Interoperability)의무화가 해제되면서 스마트폰들이 상당수 개발 되고 출시되고 있으며, 실제로 국내에 스마트폰 사용자는 2009년 말 기준 80만명에 불과했으나 11월 애

* 숭실대학교 IT정책경영학과
** 숭실대학교 컴퓨터학과 석사과정
*** 숭실대학교 컴퓨터학과 교수

플 스마트폰 도입 이후 급성장하여 20011년 4월에는 1000만명을 돌파하여 총 이동통신 가입자 5,151만명중 28.1%에 해당하는 1,145만명이 스마트폰을 사용하고 있는 것으로 나타났다[1].

<표 1> 스마트폰 가입자 현황

구 분	'09.4Q	'10.4Q	'11.1월	'11.3월	'11.4월
총가입자(만명)	4,794	5,077	5,098	5,137	5,151
스마트폰 이용자(만명) (비중 %)	81 (2)	722 (14.2)	826 (16.2)	1,038 (20.2)	1,145 (28.1)

스마트폰의 특징 중 하나인 바코드 리더 기능을 통하여 상품의 가격을 비교하거나 상품 평을 보고 상품을 구입하는 사용자가 증가하고 있고, 기존 바코드의 용량 제한을 극복하기 위해 그 형식과 내용을 확장한 2차원 형태의 코드로 구성되어 있는 QR-Code로 다양한 정보를 제공하고 있는 서비스 역시 확산되고 있다.

본 논문에서는 스마트폰의 바코드 리더 기능에서 착안하여 QR-Code를 해독해 추출한 정보와 사용자의 스마트폰 정보를 연산하여 기존의 패스워드 방식, 스마트카드, 생체 인식, 음성인식 등의 사용자 인증 기법과 달리 그 절차를 간소화하고 보안성을 강화하는 새로운 사용자 인증 기법을 설계하였다. 2장에서는 QR-Code와 기존의 사용자 인증 기법에 대해서 분석하고, 3장에서는 QR-Code를 이용한 새로운 사용자 인증 기법을 제안한다. 4장에서는 제안된 시스템을 기존 시스템과 비교하여 성능 및 보안성을 분석하고 마지막으로 5장은 결론으로 마무리 하였다.

Ⅱ. 관련연구

2.1 QR-Code

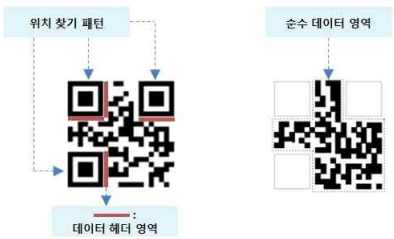
QR-Code는 흑백 격자 무늬 패턴으로 정보를 나타내는 매트릭스 형식의 2차원 바코드이다. QR-Code는 주로 일본에서 많이 사용되며 명칭은 덴소 웨이브의 등록상표 Quick Response에서 유래하였다[2].

QR-Code는 종래에 많이 쓰이던 바코드의 용량 제한을 극복하고 그 형식과 내용을 확장한 2차원의 바코드로 종횡의 정보를 가져서 숫자 외에 문자의 데이터를 저장할 수 있으며, 보통 디지털 카메라나 전용 스캐너로 읽어들여 활용되고 있다. 그 형태는 다음과 같이 2차원 행렬의 구조로 데이터를 표현하며, 크기는 버전마다 다르다.

<그림 1> QR code

QR-Code의 특징은 QR(Quick Response)이라는 명칭과 같이 디코딩 속도가 매우 빠르며, 바코드에 비하여 대용량의 데이터를 고밀도로 기록할 수 있다. 기록할 수 있는 데이터의 용량은 숫자의 경우 최대 7,089자, 숫자와 영문자의 혼합 4,296자, 이진 바이너리 2,953자, 한글이나 한자와 같은 문자의 경우 1,817자까지 기록이 가능하다. 또한 코드의 일부가 훼손되었거나 잘못 읽었을 경우 오류 정정 기능을 통하여 최대 30%까지 복원이 가능하며, 기록할 데이터의 용량에 따라 구조의 확장이 용이하다.

QR-Code의 구조는 다음과 같다.



<그림 2> QR-Code의 구조

<그림 2>와 같이 위치 검출패턴, 타이밍 패턴, 데이터 영역, 형식정보 영역으로 구성된다. 위치 검출 패턴과 타이밍 패턴은 고정되어 있는 부분으로 코드 디코딩시 위치 감지 및 좌표 결정에 사용되며, 데이터 영역과 형식정보 영역은 인코딩 된 데이터의 값에 따라 정해진다.

2.2 사용자 인증 기법

사용자 인증 기법은 임의의 정보에 접근할 수 있는 주체의 능력이나 주체의 자격을 검증하는 것으로 시스템이 접근을 요청한 사용자가 그 본인임을 인정해 주는 모든 과정을 의미한다. 이러한 인증은 해당 서비스를 사용하고자 하는 사용자 인증과 전달되는 정보에 변경이 없음을 보장하는 메시지 인증으로 구분되며 패스워드, 인증서, 생체인증 등과 같은 기술의 안전성에 의존한다.

기밀성은 권한이 없는 사람으로 하여금 해당 정보를 확인 할 수 없도록 하는 기술로서 대칭키 암호화 또는 비대칭 키 암호화 알고리즘에 기반을 두고 있다. 이러한 기밀성은 비밀키를 이용하여 정보를 암호화함으로써 정보가 노출되더라도 비밀키를 소유하지 않은 사람은 그 내용을 알 수 없도록 하는 것이 주요 목적이다.

무결성은 송·수신 되는 정보에 대하여 변경됨이 없음을 보장하기 위한 기술이다. 즉, 정보의 변경은 인가된 자에 의해서 인가된 메커니즘을 통해서만 이루어 져야 한다는 것으로 이러한 무결성은 MD(Message Digest), SHA(Secure Hash Algorithm)와 같은 해쉬 함수의 안정성에 의존 한다.

부인방지 기술은 송·수신자 상에 전송된 정보에 대해 송신하거나 수신한 사실을 부인할 수 없도록 하는 것으로 전자서명을 통해 구현될 수 있다. 이러한 부인방지 기술은 송신자의 개인키를 이용해 정보 전송 사실을 보장하는 송신 부인방지(Non-Repudiation of Origin), 신뢰할 수 있는 제 3 자에 의해 송신자의 정보가 수신자에게 전달되었음을 보장하는 전달 부인방지(Non-Repudiation of Delivery), 신뢰할 수 있는 제 3 자에게 정보가 제출되었음을 보장하는 제출 부인방지(Non-Repudiation of Submission), 마지막으로 수신자에게 정보가 전달되었음을 보장하는 수신 부인방지(Non-Repudiation of Receipt)등이 있다[3, 4]. 이러한 부인방지 기술은 적용되는 방식에 따라 대칭 방식[5, 6]과 비대칭 방식으로 구분할 수 있다.

사용자가 인증서버에 자신이 누구임을 밝히는 식별(Identification), 인증 서버가 접근을 요청하는 사용자를 증명하는 인증(Authentication), 접근이 허용된 사용자에 대해 접근통제 메커니즘에 입각해 시스템 자원 사용을 허가하는 권한부여(Authorization) 단계로 이루어진다. 특히, 인증 과정은 접근 요청자가 서비스 제공자로부터 제공되는 서비스를 제공받기 위해서는 필수적인 요구 조건이다.

사용자 인증 기법은 형태에 따라서 다음에서와 같이 사용자가 알고 있는 것을 인증 요소로 사용하는 Type-I 인증, 사용자가 소유하고 있는 물건을 인증 요소로 사용하는 Type-II 인증, 사용자의 신체적 특징을 이용하는 Type-III 인증, 사용자의 행동적 특징을 이용하는 Type-IV 인증으로 분류할 수 있다[7].

<표 2> 인증 요소에 따른 형태 분류

Classification	Description	Example
Type Ⅰ Authentication	Something you know	Password, PIN
Type Ⅱ Authentication	Something you have	Smart card, Token
Type Ⅲ Authentication	Something you are	Iris, Fingerprint
Type Ⅳ Authentication	Something you do	Voice, Signature

2.2.1 패스워드 방식

현재 가장 많이 사용되는 인증 메커니즘은 패스워드 인증이다. 패스워드 인증은 사용하기 쉽고 가격이 다른 메커니즘에 비해 저렴하다는 이유로 패스워드 기반의 인

증 메커니즘이 가장 널리 이용된다. 하지만 다수의 사용자들이 이름이나, 생일 취미 등과 같은 자신과 직접 또는 간접적으로 연관된 정보들을 패스워드로 이용한다는 점에서 추측하기 쉽고, PWDUMP[8], NT Crack[9], John the Ripper[10]와 같은 소프트웨어에 의해 쉽게 깨질 수 있다는 문제점이 존재 한다. 또한, 원격 접속 시 패스워드가 평문으로 전송될 경우 스니핑 공격의 대상이 되어 패스워드가 노출될 수도 있고, 무차별 공격에 의해 결국에는 패스워드가 깨진다는 단점이 존재 한다[11].

2.2.2 스마트카드 방식

스마트카드는 가로 85.6mm, 세로 54mm, 두께 0.76mm 등의 물리적 특성을 가지고 있으면 스마트카드 내부에는 마이크로프로세서, 카드 운영체제, 보안 모듈, 메모리 등을 갖추고 있다. 이러한 스마트카드는 리더와의 접촉 유·무에 따라 접촉식 카드[12]와 비 접촉식 카드[13]로 구분된다.

2.2.3 생체 정보 방식

생체 인증은 사용자를 인증하기 위하여 지문이나 홍채, 정맥과 같은 개인의 생체적 특징이나 혹은 서명, 음성, 키보드 입력등과 같은 개인의 행동적인 특성을 이용하는 방법이다. 그러나 주변 환경에 따라 인식률의 차이 그 급격하고, 종교 및 문화적 차이에 따른 사용 거부감 등이 문제로 제기되고 있다. 또한 초기 도입 비용이 상당히 비싸기 때문에 비용대비 효과성에 대한 의문이 계속해서 거론되고 있는 실정이다.

2.2.4 공인인증서 방식

공개키 기반 구조(PKI : Public Key Infrastructure)인 증서를 이용하여 사용자를 인증하는 방법으로 현재 대부분의 시스템에서 적용하여 사용되어지고 있다. 이 방법은 사용자 인증 기능 외에도 전자서명 기능도 함께 제공하고 있으며, 인증서 발급 및 등록, 사용자 등록 인증서 검증과정을 거쳐 사용자를 인증하게 되는 방법이다[14, 15].

공인인증서를 이용한 사용자 인증의 단계에는 크게 인증서 발급 및 등록과정, 사용자 등록 과정, 인증서 검증 과정으로 나눌 수 있는데, 공인인증 체계에서는 대면 확인을 거쳐 높은 보안 수준을 유지한다. 이를 위해 사용자는 인증서 등록과정에서 개인의 주민등록번호, 서비스를 제공하는 사용자의 경우는 법인번호를 인증기관(CA : Certificate Authority)에게 제공해야 한다. 이를 통해 인증기관은 사용자에 대한 신원정보를 확보하게 되고 이를 토대로 인증서를 발급하게 된다. 특히 사용자 신원정보는 인증서를 식별할 수 있는 정보로 사용된다[16].

Ⅲ. QR-Code를 이용한 새로운 사용자 인증 기법

이 장에서는 QR-Code를 이용한 새로운 사용자 인증 기법에 대해 구체적으로 설명하고, 세부 프로토콜을 제안한다.

제안하는 방식은 다음과 같은 조건을 만족해야 한다.

(1) 사용자는 QR-Code를 촬영하기 위해 카메라가 탑재된 스마트폰을 소지하고 있어야한다.
(2) 사용자는 이용하려는 서비스에 가입되어 있어야 하며, 단말의 정보가 정상적으로 입력되어 있어야 한다.
(3) 서비스 서버에 등록되어 있는 사용자 단말의 정보는 인가된 클라이언트를 통해서만 변경이 가능하다.
(4) 단말에는 인증 어플리케이션이 설치되어 있어야 한다.
(5) 단말은 암·복호화 및 연산을 위하여 SHA-1 해시 함수와 AES 알고리즘을 수행할 수 있는 연산능력을 가지고 있어야 한다.

3.1 제안 시스템

제안하는 시스템은 사용자가 인가되지 않은 다양한 장비를 통해 서비스에 접근할 수 있기 때문에 발생하는 보안 위협을 방지하기 위해 기존의 사용자 인증 기법을 사용하지 않고 스마트폰을 이용한 새로운 사용자 인증 기법이다.

<그림 3> 제안하는 시스템 전체 구성도

사용자가 외부에서 서비스에 접근할 때 클라이언트에서 인증정보(아이디 및 패스워드 등)를 입력하는 것이 아닌 단말을 통해 클라이언트를 대신 인증 하는 방식으로 비 인가된 클라이언트에 인증을 위해 필요한 어떤 정보도 입력하지 않아 기존의 인증시스템에서 발생할 수 있는 보안 문제점을 해결하는 방식으로 안전하게 사용자 인증을 할 수 있다.

Step 1. 사용자가 외부에서 인가되지 않은 클라이언트를 통해 서비스 제공자에게 서비스 접근 요청한다.

Step 2-3. 서비스 제공자는 외부 접근 요청을 한 클라이언트의 정보를 추출한 뒤, QR-Code를 생성한 후 클라이언트로 전송한다.

Step 4-7. 클라이언트 화면에 QR-Code가 나타나면 사용자는 등록된 단말로 QR-Code를 스캔하여 분석 후, 서비스 제공자에게 클라이언트 인증을 요청한다.

Step 8. 클라이언트 인증을 요청 받은 서비스 제공자는 스마트 폰을 인증 후 클라이언트를 인증하여 서비스를 제공한다.

3.2 사용자 인증 프로토콜

외부에서 인가되지 않은 클라이언트를 통해 서비스 접근을 할 경우 서비스 제공자는 접근을 시도한 클라이언트의 정보를 추출하여 QR-Code를 생성하여 클라이언트에 전송하고 단말로 QR-Code를 스캔하여 사용자 인증단계를 거치게 된다. QR-Code 생성 프로토콜과 인증 프로토콜로 구분하여 제언한다.

다음은 상세 프로토콜에서 쓰이는 약어를 정리한 것이다.

<표 3> 약어 정리

약어	설명
ME_i	$H(PN \oplus ID)$
PN	이동통신사로부터 부여받은 사용자 전화 번호
ID	단말에 기 입력되어 있는 사용자 아이디
PW	단말에 기 입력되어 있는 사용자 패스워드
RSN	Random Serial Number
Key	AES 128 bit Key
$H()$	해시함수
TS	타임스탬프

3.2.1 QR-Code 생성 프로토콜

다음과 같은 단계를 거쳐 QR-Code를 생성하여 클라이언트에게 전송한다.

Step 1. 클라이언트가 외부 접근을 요청한다.

서비스 제공자는 클라이언트의 일반 정보(Client IP Address, Mac Address, Web Browser 등)를 추출한다. 추출한 클라이언트 정보를 연산하여 CI를 생성한다.

$$CI : H(Client\ Information) \quad (1)$$

후에 단말이 인증 요청할 때, 클라이언트와 매칭하기 위해 필요한 *RSN(Random Serial Number)*과 QR-Code에 있는 내용을 AES 알고리즘을 이용하여 암·복호화할 때 사용하기 위한 *Key*를 생성한다.

QR-Code를 생성할 때 데이터로 들어갈 *Enc-Value*를 *RSN*과 *CI*를 XOR하여 *Key*로 암호화하여 생성한다. 이때 암호화 이유는 데이터(Client Information)의 변경을 방지하기 위함이다.

$$Enc\_Value : E_{KEY}(H(RSN \oplus CI)) \quad (2)$$

데이터로 사용되는 값들을 모두 생성 한 뒤 QR-Code를 생성한다. QR-Code에는 데이터로 *ENC_Value, RSN, TS* 와 *CI* 를 이용하여 생성된다.

$$QR\text{-}Code : ENC\_Value||RSN||TS||CI \quad (3)$$

Step 2. 생성된 QR- Code를 클라이언트에 전송한다.

Step 3. 클라이언트는 주기적으로 서비스 제공자에게 단말을 통해 인증이 완료 되었는지 확인 요청한다.

3.2.2 인증 프로토콜

사용자는 QR-Code를 스캔하여 다음과 같은 단계를 거쳐 단말을 인증 한 뒤 클라이언트의 외부 접근을 허가한다.

Step 1. 단말은 클라이언트의 화면에 있는 전송받은 QR-Code를 스캔한 뒤 내용을 분석하여 나온 클라이언트의 정보와 실제 클라이언트의 정보가 일치하는지 확인한다.

Step 2. 단말은 QR-Code를 서비스 제공자가 생성하였는지 확인하기 위해 QR-Code의 데이터 중 *RSN, TS* 그리고 *PN*을 연접하여 RRC(Request *RSN* Confirm)을 생성하여 서비스 제공자에 전송한다.

$$RRC : RSN || TS || PN \quad (4)$$

서비스 제공자는 전송받은 RRC에서 *RSN*의 유효성을 확인한 후 *PN*과 매칭되는 미리 연산해 둔 ME_I 를 확인한다.

Step 3. 서비스 제공자는 자신이 QR-Code를 생성하였다는 것을 확인 시켜 주기 위해 RRS(Response *RSN* Confirm Server)를 생성하고, *TS*와 *Key* 값을 RRS와 함께 단말기에게 전송한다.

$$RRS : H(RSN \oplus MEI \oplus Key) \quad (5)$$

단말은 RRS를 검증하기 위해 자신이 가지고 있는 *PN*과 *ID*를 연산해 ME_I를 생성한 후, RRS와 동일한 메시지를 생성하여 전송받은 RRS와 비교 검증한다.

$$\text{Compare RRS with } (H(RSN \oplus ME_I \oplus Key)) \quad (6)$$

RSN의 유효성을 확인한 단말은 QR-Code의 Client Information의 무결성을 검증하기 위해 *CI*를 생성하여 *RSN*과 연산처리를 한다. 그 후 QR-Code의 데이터 중 하나인 *Enc_Value*와 비교 검증을 한다. 비교 검증이 끝나면 QR-Code

의 무결성 검증이 완료됨으로써 단말은 서비스 제공자를 인증하게 된다.

Compare
DKey(Enc_Value) with H(RSN⊕CI) (7)

Step 4. 서비스 제공자에 대한 인증이 완료 된 후, 단말은 자신을 인증하기 위해 UID(User Identity Data)를 생성하여 *RSN*, *PN*, *TS* 를 함께 서비스 제공자에게 전송한다.

UID : H(MEI⊕PW⊕TS⊕RSN) (8)

Step 5. 모든 검증과정이 끝난 후 서비스 제공자는 클라이언트의 외부 접근을 허가 한다.

Ⅳ. 성능 분석 및 평가

제안한 새로운 사용자 인증 기법의 효율성과 성능을 알아보고, 기존의 사용자 인증 시스템과의 비교 분석을 수행함으로써 보안의 우수성을 알아본다.

4.1 보안 요소 분석

4.1.1 인증(Authentication)

사용자는 서비스 제공자가 생성한 QR-Code의 무결성을 *RSN*과 *Key* 값을 통해 검증하고, 서버는 사전에 등록한 단말의 정보를 검증하여 인증하기 때문에 정당한 사용자만 서비스를 이용할 수 있다.

4.1.2 기밀성(Confidentiality)

송수신 되는 데이터는 노출에 대한 위험이 없는 데이터를 제외하고는 송수신 측에서 연산처리가 가능한 데이터를 생성하여, 여러 데이터를 연접하여 해시 절차를 통해 데이터가 전송되기 때문에, 도청 및 개인정보 유출로부터 안전하다.

4.1.3 무결성(Integrity)

기밀성과 비슷하게 실질적으로 전송되는 데이터는 모두 해시 절차를 통해서 전송되기 때문에, 중간자로부터 데이터가 변조되는 공격을 방지할 수 있다. QR-Code의 무결성 검증은 *RSN*과 *Key* 값을 통해 검증이 가능하여 더욱 신뢰성을 높일 수 있다.

4.1.4 가용성(Availability)

복잡한 연산을 통해 여러 인증기관을 경유하는 시스템이 아니며, 연산처리가 복잡하지 않은 해시 연산과 AES 연산만 사용하여 처리속도가 빠르다. 또한, 재전송이나 서비스 거부 공격 등에 대해서도 *RSN*과 *Key*의 유효시간을 통해 해결 가능하여 가용성이 뛰어나다.

4.2 안전성 비교 분석

기존의 사용자 인증 시스템과 제안 시스템의 안전성은 아래와 같다.

<표 4> 안전성 비교 분석

	id /password	공인인증서	제안시스템
패스워드 추측 공격	가능	불가능	불가능
패킷 스니핑	가능	불가능	가능
중간자 공격	가능	가능	불가능
재전송 공격	가능	가능	불가능
위조 공격	가능	불가능	불가능
키보드 해킹	가능	가능	불가능
웹사이트 해킹	가능	가능	불가능

4.2.1 패스워드 추측 공격

기억하기 쉬운 정보들을 포함하거나, 짧은 문장으로 이루어진 패스워드를 다양한 사용자가 사용을 하고 있다. 이러한 패스워드는 사용자가 자주 사용하는 정보를 이용하여 악의적인 제 3자의 추측에 의해서 획득이 가능하다. 그러나 제안한 인증 기법에서는 패스워드를 최종적으로 전송할 때, H(MEI⊕PW⊕TS⊕RSN) 연산을 통해 전송하기 때문에, 암호학적 해시함수의 일방향성 때문에 패스워드의 추측이 어렵다. 또한, 패스워드를 추측 하였더라도 그 외의 값들을 알 수 없어 서비스 제공자로부터 최종적인 인증이 불가능하다.

4.2.2 패킷 스니핑

모든 정보나 메시지, 인증 데이터는 패킷 전송을 통해 이루어진다. 따라서 정보가 담긴 패킷을 악의적인 3자에게 공격을 당한다면, 텍스트 형태로 전송되는 메시지나 정보는 그대로 노출이 된다. 제안하는 인증 기법에서 사용자와 서비스 제공자간의 데이터를 공격자에게 다 노출당한다고 하더라도, 전송되는 데이터에서 알아 볼 수 있는 내용은 공격자에게 알려져도 위협이 없는 데이터이며, 알려져서는 안 되는 데이터는 연접 되어 해시 함수를 사용하기 때문에, 해시 함수의 일방향성 때문에 패킷의 내용이 노출되지 않아 스니핑 위협에서 벗어날 수 있다.

4.2.3 중간자 공격

공격자는 사용자와 서비스 제공자 사이에서 패킷을 가로채 중간자 공격이 가능하다. 제안하는 인증기법에서 예를 들면, 공격자가 서비스 제공자에게 접근하여 QR-Code를 받고, 접근하는 사용자에게 공격자가 서비스 제공자에게 받은 QR-Code를 전송한다. 사용자는 전송받은 QR-Code를 통해 서비스 제공자에게 인증을 받으면, 공격자의 접근이 허가가 되는 방식으로 공격을 할 수 있다. 하지만 제안하는 인증 기법 에서는 QR-Code의 데이터 검증을 통해 중간자 공격을 막을 수 있다. QR-Code의 클라이언트 정보가 수정이 될 경우, 해시 함수를 통해 생성한 값과 달라 검증이 안 되기 때문에, QR-Code의 변경이 파악 되어, 중간자 공격이 불가능하다.

4.2.4 재전송 공격

일반적으로 서버의 인증을 받기 위한 사용자의 인증 데이터는 고정되어 있다. 기존 사용자가 접속 하고 있거나, 접속 종료 후 악의적인 3자가 동일한 인증 데이터를 가지고 사용자를 가장하여, 서버의 인증을 받을 수 있다. 그러나 제안하는 인증 기법에서는 공격자가 인증 데이터를 획득하더라도, 인증 데이터에 속하는 RSN 값이 가진 유효시간으로 인해 인증데이터는 무용지물이기 때문에, 서비스 제공자로부터 재전송 공격을 통한 인증이 불가능하다.

4.2.5 위조 공격

악의적인 공격자가 사용자의 인증데이터를 위조하여 서버의 인증을 얻기 위한 공격 기법으로, 서버에서는 올바른 인증 데이터를 선별해야 하며, 기존의 등록된 사용자의 인증 정보를 가지고, 재등록 및 인증을 하지 못하게 해야 한다. 제안하는 인증 기법에서는 기존의 등록된 사용자의 인증정보를 공격자가 획득하더라도 RSN 과 Key 값의 유효 시간으로 인해 사용할 수 없어 위조 공격이 불가능하다.

4.2.6 키보드해킹, 웹사이트 해킹

공격자는 사용자의 클라이언트에 악의적인 프로그램을 심어놓고, 사용자의 키보드를 해킹할 수 있으며, 웹사이트를 해킹하여 피싱을 할 수 있다. 하지만 제안하는 인증 기법에서는 인증을 위해 사용자의 클라이언트에 입력하는 어떠한 값도 없으며, 웹 사이트가 해킹 되더라도,

단말을 통해 최종 인증을 하기 때문에 키보드 해킹과 웹 사이트 해킹의 위협에서 벗어날 수 있다.

4.3 효율성 분석

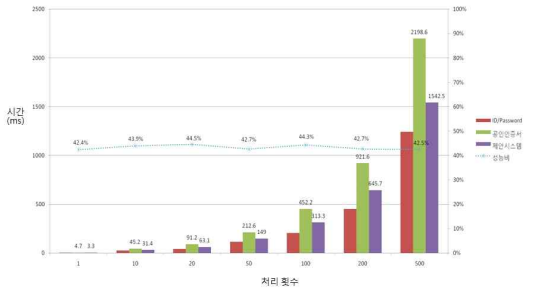
기존의 인증 기법과 제안 기법의 효율성을 비교 분석하기 위해 클라이언트의 처리시간을 비교 분석 하였다. 공인인증서 방식은 클라이언트에서 메시지를 SHA1 알고리즘을 사용하여 해시 값을 추출하고 세션키를 생성한 뒤, 메시지 원본과 해시 값 세션키를 연접한 평문을 서버의 공개키로 암호화하여 나온 값을 디지털 서명을 위해 사용자의 개인키로 암호화하는 방식의 테스트 모듈을 만들어 처리 시간을 테스트하였다.

제안시스템 역시 클라이언트에서 행하는 해시 및 복호화를 하는 테스트 모듈을 만들어 처리시간을 테스트 하였다. 테스트 모듈의 환경이 PC였기 때문에 스마트폰의 사양보다 훨씬 높아 한번의 동작으로는 차이가 미세하여, 정확한 효율성분석을 위해 기존 시스템의 동작 횟수와 제안 시스템의 동작 횟수를 늘리게 되면 차이를 알 수 있다. 각 횟수마다 100번의 테스트를 통해 평균 값을 표로 만들었다.

<표 5> 효율성 비교 분석

구분	ID/Password	공인인증서	제안시스템
1회	2.4 ms	4.7 ms	3.3 ms
10회	24.9 ms	45.2 ms	31.4 ms
20회	43.7 ms	91.2 ms	63.1 ms
50회	115.6 ms	212.6 ms	149.0 ms
100회	205.1 ms	452.2 ms	313.3 ms
200회	453.2 ms	921.6 ms	645.7 ms
500회	1243.6 ms	2198.6 ms	1542.5 ms

위의 표에서 보면 제안 시스템보다 안전성이 낮은 인증시스템인 ID/Password 방식보다는 느린 속도를 보이지만 공인인증서 인증 시스템보다는 빠른 속도를 보이고 있다.



<그림 4> 기존 시스템과 제안 시스템 효율성 비교분석 그래프

Ⅴ. 결론

본 논문에서는 인가되지 않은 클라이언트를 통해 서버에 접근하는 사용자에 대해 스마트폰을 통해 안전하게 인증할 수 있는 방안으로서, 상호 인증을 하고 기존의 인증 기법의 문제점 해결에 대한 연구를 하였다.

기존의 인증 방식은 해킹의 위협이나 정보 분실 시 발생하는 위험도가 높은 취약성이 존재하지만, 제안하는 시스템은 클라이언트에서 아무런 입력을 하지 않고 스마트 폰을 통해 사용자를 인증 할 수 있는 값을 생성해 내기 때문에 기존의 인증 방식 보다 안정성이 뛰어남을 확인하였고, 또한 기존의 인증방식은 대부분 사용자만 인증하는 일방향성 인증으로 피싱 공격 등 위협이 있지만, 제안하는 방식은 양방향으로 상호 인증을 하기 때문에 보안 위협에서 벗어날 수 있다. 기기의 도난 및 분실 문제에서도 분실인지가 가장 빠른 단말을 사용함으로서, 다른 장비의 분실보다 빠르게 인지하여 신고 할 수 있고, 분실을 인지하지 못하더라도 단말 내부 패스워드를 통해 공격자 접근을 방지할 수 있다.

효율성 부분 역시 비교 분석에서 보는 바와 같이 기존의 인증기술보다 빠르거나 뒤처지지 않음을 확인 할 수 있다. 따라서 처리 연산 부분이 빨라 공인인증서 방식보다 약 43.3%의 성능 향상이 있고, ID/Password 방식보다는 효율성이 낮지만 보안강도가 더 높은 것을 확인할 수 있다.

향후에는 단말 정보가 아닌 사용자의 고유한 정보로 인증 데이터를 대체 할 수 있는 연구가 필요하다. 그러기 위해서는 아직까지 알려지지 않은 공격 유형에 대한 연구 및 분석이 필요할 것이다.

참고문헌

[1] 방송통신위원회, "이동통신요금인하방안발표자료," 보고서, 06, 2011.

[2] Denso-Wave, About 2D Code | QR-Code. com Retrieved 2009-04-23.

[3] ISO/IEC 13888-1 : General model

[4] 윤승구, 박재표, "OTP를 이용한 인터넷뱅킹 시스템의 다중 채널 인증 기법," 디지털산업정보학회지, 제6권, 제4호, 2010, pp.131-142.

[5] ISO/IEC 13888-2 : Mechanism using symmetric techniques

[6] 이영숙, 김지연, "스마트폰 보안 기술 분석," 디지털산업정보학회지, 제6권, 제2호, 2010, pp91-105.

[7] Forouzan, "Cryptography and Network Security," McGraw-Hill, 2007.

[8] PWDUMP6 Version1. 7. 2, 2008., "URL source :http://www.foofus.net/fizzgig/pwdump/downloads.htm/"

[9] Bugtraq: ANNOUNCE : NTCrack v2.0., "URL source : http://seclists.org/bugtraq/1997/Mar/0103.html/"

[10] Solar Designer. John the ripper, "URL source : http://www.Openwall.com/john/"

[11] 박왕성, 정종필, 박창섭, 이동훈, "패스워드를 이용한 인증 프로토콜들에 대한 고찰," 한국정보보호학술학회지, 제9권, 제4호, 1999, pp.51-63.

[12] ISO7816 Standard Smart-Card Interface

[13] ISO14443 Type A/B Comportable., Read&Writer API Header in C

[14] 김지홍, "인증기술," 정보통신망 정보보호워크샵 발표지, 제5집, 1999, pp.187-252.

[15] 최은정, 김찬오, 송주석, "공개키 암호 기법을 이용한 패스워드 기반의 원거리 사용자 인증 프로토콜," 한국정보과학회논문지, 정보통신 제30권 제1호, 2003, pp.75-80.

[16] Radia Perlman, "An Overview of PKI Trust Models, IEEE Network," Vol. 13, No. 6, pp. 38-43, November/December 1999.

■ 저자소개 ■

이 용 재
Lee, Yong Jae

2011년 5월~현재
현대자산운용 대표이사
2011년 3월 숭실대 IT경영정책학 박사과정 수료
2000년 12월 KAIST K-CEO 과정 수료
1984년 8월 연세대학교 교육대학원 교육학 석사
1982년 2월 숭실대학교 법학과 졸업

관심분야 : 증권 관련 정보보호
E-mail : yjlee@hyundaiam.com

김 영 곤
Kim, Young Gon

2009년 9월 ~ 현재
숭실대학교 일반대학원 컴퓨터학과 석사과정

관심분야 : 정보보호, 네트워크 보안, 인증
E-mail : kyg994@gmail.com

박 태 성
Park, Tae Sung

2009년 9월 ~ 현재
숭실대학교 일반대학원 컴퓨터학과 석사과정

관심분야 : 정보보호, 네트워크 보안, PKI
E-mail : glittering87@naver.com

전 문 석
Jun, Moon Seog

1991년 3월~현재
숭실대학교 정교수
1989년 9월~1991년 2월
NMSU, PSL 연구소 책임연구원
1989년 3월~7월
Morgan State University 조교수
1986년 9월~1989년 12월
of Mary 강사
1989년 2월 University of Maryland Computer Science 박사
1986년 2월 University of Maryland Computer Science 석사
1981년 2월 숭실대학교 전산과 졸업

관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학
E-mail : mjun@ssu.ac.kr

논문접수일 : 2011년 8 월 5 일
수 정 일 : 2011년 8 월 28 일
게재확정일 : 2011년 9 월 5 일