# SMS와OTP에기반한사용자인증시스템설계및구현

김우경*, 서선희*, 이경현**
*부경대학교 전산정보학과
**부경대학교 전자컴퓨터정보통신공학부
e-mail:carygun@empal.com

# DesignandImplementationofaUser AuthenticationSystemBasedonSMSand OTP

Woo Kyung Kim*, Sun Hee Seo*, Kyung Hyun Rhee**
*Department of Computer and Information Science , Pukyung National University
**Devision of Electronic, Computer & Telecommunication Engineering, PuKyong National University

**요 약**

인터넷을 통한 자동화된 업무가 증가함에 따라서, 공공 컴퓨터들에 대한 의존도가 높아지고 있다. 그러나 오늘날 웹메일, 옥션, 인터넷 뱅킹, 휴대폰 결제등과 같은 위한 원격 서비스들은 사용자의 신원을 증명하기 위해 사용자의 아이디와 패스워드 또는 주민등록번호를 요구한다. 하지만 안전하지 못한 채널로 전송되는 사용자의 정보는 공격자에 의해서 도청및 재사용될 가능성이 매우 높다. 본 논문에서는 위와 같이 보안이 취약한 환경에서 안전한 사용자 인증이 성공적으로 이루어 질 수 있는 새로운 인증 시스템을 제안하고자 한다. 제안 시스템은 현대의 일반 사용자들이 항상 소지하는 휴대폰의 SMS(Simple Message Service)와 일회용 패스워드(OTP : One Time Password)를 기반으로 한다.

## 1. 서 론

인터넷을 통하여 안전한 업무나 상거래를 수행하기 위하여 전송되는 정보를 악의적인 사용자들로부터 보호하기 위한 여러 가지 보안 기술들이 연구되고 있으며, 인터넷을 통한 사용자 인증 기술은 크게 두 가지로 분류될 수 있다.

- 공인 인증서(Certificate)를 통한 인증
- 아이디/패스워드를 통한 인증

첫째로, 공인 인증서를 통한 인증시스템은 사용자의 성공적인 인증을 수행하기 위해서 사용자는 항상 자신의 공인 인증서와 대응되는 비밀키를 자신의 휴대용 장치에 안전하게 보관하고 사용해야만 한다. 또한, 사용자가 악의적인 컴퓨터를 사용하여, 공인 인증서를 통한 인증을 수행할 시에 악의적인 컴퓨터로부터 사용자의 비밀키 노출을 방지하기가 어려운 단점이 존재한다. 둘째로, 아이디/패스워드를 통한 인증 시스템은 가장 고전적인 접근 방법으로 사용자의 기억능력에 기반하며, 언제 어디서나 쉽게 성공적인 인증을 수행할 수 있다. 하지만, 도청, 재사용, 오프라인 사전등과 같은 공격에 취약하다. 실질적 인터넷 환경에서는 이러한 도청과 재사용을 방지하기 위하여, 서버 인증만을 수행하는 SSL(Secure Socket Layer)를 통한 안전한 채널을 생성함으로써, 전송되는 아이디, 패스워드에 대한 공격들을 방지하고 있다. 하지만, 이러한 접근법은 실질적인 주가 되는 아이디/패스워드를 통한 인증의 취약점을 보완하기 위한 또 다른 보안 기술인 SSL을 중복적으로 사용함으로써 적절한 보안성을 만족시키는 형태로 볼 수 있다.

따라서, 본 논문에서는 소개된 시스템들에서의 악의적인 컴퓨터로부터 사용자 비밀정보에 대한 도청과 재사용을 방지할 수 있는 새로운 사용자 인증

시스템을 제안하고자 한다. 제안 방안은 휴대폰에서 사용되는 SMS와 S/Key와 같은 일회용 패스워드(OTP)기술을 기반 하고 있다. 본 논문의 구성은 아래와 같다. 제2장에서는 관련연구를 소개하고, 제3장에서는 새로운 사용자 인증 시스템에 대한 소개와 구현결과를 소개하며, 제4장에서는 결론을 맺는다.

## 2.관련연구

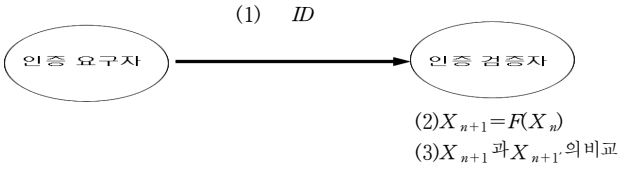
### 2.1 일회용 패스워드 동기화 방식

일회용 패스워드 메커니즘은 서버와 클라이언트(또는 토큰) 사이에 미리 약속된 규칙에 의해서 클라이언트 쪽에서 생성한 일회용 패스워드를 서버로 전송하면 서버 또한 동일한 규칙에 의해 사용자 데이터가 들어있는 데이터베이스에서 비밀값을 가져온 후, 일회용 패스워드의 유효성을 검사하는 방식이다.

본 논문에서 소개하는 일회용 패스워드 메카니즘인 S/Key는 시도/응답(Challege/Response)방식을 사용하고 있으며, 전체적인 보안성은 일방향 해쉬함수(Cryptographic Hash Function)에 기반하고 있다.

안전한 일방향 해쉬함수의 조건은 한쪽 방향으로는 계산하기 쉽지만 그 역방향으로는 계산하는 것은 사실상 불가능한 것이다. 즉, 입력값 $X$와 출력값 $Y$를 갖는 안전한 해쉬함수 $F$는 $Y=F(X)$와 같이 나타낼수 있으며, 주어진 $X$로부터 $Y$를 계산하는 것은 빠르고 쉽지만, 주어진 $Y$에서 $Y=F(X')$인 $X'$를 찾는 것은 매우 어렵다.

S/Key에서는 $2^{64}$ (약 $10^{19}$)의 값들을 가지는 해쉬함수를 사용하며, 기본적으로 MD4 해쉬함수를 사용한다. 최근의 연구결과에서 MD4가 안전하지 않은 것으로 판명되어 MD5 또는 DES-MAC 등을 사용하는 시스템도 등장하고 있다[1]. 기존의 S/Key 일회용 패스워드 생성 매커니즘은 그림 1에서 나타난 바와 같이 일방향 함수를 사용하여 인증정보인 일회용 패스워드를 생성한다.




<그림 1> 일방향 함수를 사용한 기존 일회용 패스워드 매커니즘

여기에서는 최초 난수 $R$값을 생성하고 이 값에 대해 $X_{n+1}=F^n(F(PW|R))$이 되도록 일방향 함수 $F$를 $n+1$번 수행하여 $X_{n+1}$를 구한다. 여기서, PW는 인증요구자의 패스워드이다. 그리고 $R$과 $X_{n+1}$을 인증검증자 시스템 최초 설정시 전달하여 저장해둔다.

인증 요구자가 검증자에게 인증을 받을 필요가 생기면, 그림 1의 (1)에서처럼 자신의 패스워드와 $R$값에 일방향 함수 $F$를 $n$번 수행한 $X_n$을 인증 정보로 인증 검증자에게 전달하게 된다. (2)에서 인증 검증자는 전달 받은 인증 정보의 $X_n$을 이용하여 일방향 함수 $F$를 1회 더 계산함으로써 $X_{n+1'}=F(X_n)$을 구한다. (3)에서 인증 검증자는 앞서 계산된 $X_{n+1'}$ 값을 시스템 설정시 저장한 $X_{n+1}$ 값과 비교하여 같으면 인증 요구자를 인증하게 된다. 인증이 성공적으로 이루어지게 되면 인증 검증자는 다시 $X_n$을 저장한다. 그림 2는 S/Key 일회용 패스워드 생성 매커니즘에서 인증 정보를 생성하기 위해 인증 요구자와 검증자가 각각 일방향 함수를 어떻게 사용하는지 구체적으로 보여준다[2].

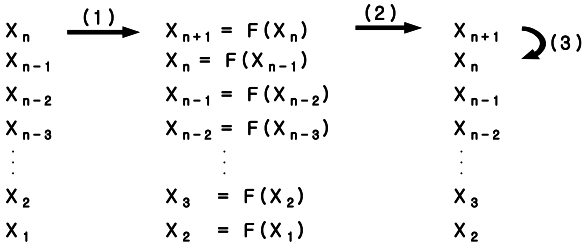



그림 2 S/Key 에서의 일방향 함수 운용 개념

### 2.2 일회용 암호 생성기 (Token)

일회용 암호 생성기는 휴대가 간편해야 하기 때문에, 명함 크기의 계산기 모양, 열쇠고리 모양, 스마트 카드, USB등의 키 형태로 만들어지며, 질의 값 또는 응답 값의 입력 및 작동 방법 등 사용이 간편해야 한다. 일반적으로 일회용 암호 시스템에 쓰이는 토큰의 경우 데이터 암복호화 기능이 필요 없기 때문에 소형으로 컴퓨터와 접속 장치 없이 단순 연산 기능, 디스플레이 기능, 버튼 인터페이스만으로 구현 된다. 또한,해체 방지 기능(tamperproof)을 위해 토큰 속의 모든 중요한 데이터는 RAM, Secure EEPROM 등에 위치하여야 하며, 해체시도 시 전원이 오프되며 그간 사용된 모든 데이터가 자동 소거되는 기능이 필수적이다. 토큰 자체 운영 프로그램도 RAM 등 휘발성 메모리에서 동작하게 하는 것이 바람직하며 최소한 외부에서 읽혀질 수 없도록 마스킹(masking)되어 사용되거나 OTP(One Time Programmable)타입일 경우 외부에서 읽기 방지가 되는 프로세서가 사용되어져야 한다. 스마트카드를 이용하는 경우는 해체 방지 기능에서 탁월한 효과를 보게 된다. 하지만 COS(Card Operating System)에 일회용 암호 알고리즘이 들어가야 하며, 별도의 접속 장치가 필요하기 때문에 많은 비용이 소모되는 단점이 있다[7]. 본 논문에서는 휴대폰을 하나의 토큰으로써 사용한다.

2.3 CDMA(Code Division Multiple Access) 방식에서의 SMS(Short Message Service) 서비스

미국 퀄컴사가 주파수 대역확산 기술을 응용하여 개발한 부호분할 다중 접속 방식의 디지털 셀룰라 시스템으로 여러 사용자가 시간과 주파수를 공유하면서 신호를 송수신할 수 있다. 즉, 여러 사용자가 동일한 주파수를 동시에 사용함으로 가입자 수용 용량을 그 만큼 늘일 수 있다. CDMA 방식은 대용량이며 고품질의 데이터 서비스 제공이 가능하며 보안성이 뛰어난 장점을 가지고 있어 현재의 셀룰러/pcs 방식의 이동통신 등의 다양한 분야에 응용되고 있는 기술이다[3][4].

SMS는 일반적으로 통화채널과는 별도로 이동통신 상에서 Paging Channel 및 Traffic Channel을 이용하여 사용자에게 메시지를 전송한다. 또한, 전달할수 있는 데이터의 양은 제한적이나, 사용자가 이동통신 시스템에 연결되지 않아도 메시지를 전달 받을 수 있는 서비스이다. 본 논문에서 사용하는 SMS는 CDMA 방식하에서는 기본적으로 보안성이 뛰어나므로 부가적인 암호화는 고려하지 않는다.

## 3. SMS와 OTP를 이용한 인증시스템 제안

3.1 구조

본 논문에서 제안하는 시스템에서, 사용자와 서버는 S/Key와 동일한 방법으로 OTP를 위한 초기화를 수행한다. 하지만, 사용자는 R값을 저장 또는 기억할 필요가 없다. 사용자가 인증을 시도할 경우, 서버는 R값과 반복수를 사용자의 휴대폰으로 SMS를 이용하여 보내게 된다. 사용자는 휴대폰에 자신만이 알고 있는 패스워드를 입력하여, 일회용 패스워드(OTP)를 만들게 된다. 그러면 사용자는 그 OTP를 PC에 입력하고, 그 값은 서버로 전달되다. 서버는 수신한 OTP검증을 통해서 사용자를 인증하게 된다.

3.2 인증 프로토콜

1) 클라이언트는 PC에 ID를 넣는다.
2) PC에서 서버로 먼저 ID가 전달된다.
3) 서버에서는 ID에 대응되는 $R$값과 반복수값을 사용자의 휴대폰에 SMS로 보내준다.
4) 사용자는 자신의 휴대폰에 날아온 SMS를 확인하고, 자신의 휴대폰에 자신의 패스워드를 입력한다.
5) 휴대폰에서 OTP를 계산한다.
6) 사용자는 휴대폰에서 계산된 OTP를 PC에 입력한다.
7) 입력된 OTP는 서버에 전송된다. 서버는 수신한 OTP에 대한 검증을 S/Key와 동일한 방법으로 수행한다.

일회용패스워드에서는 반복수가 제한적이기 때문에 초기에 설정한 반복수 만큼의 로그인 시도를 했을 경우에 다시 일회용 패스워드에 관련된 정보를 초기화 해야만 한다. 따라서, 이런한 단점을 해결하기 위해서 일회용 패스워드에 사용되는 해쉬체인을 재초기화하기 위해 서명기법(OTS: One Time Signature)를 사용하는 [5]의 기법을 적용 가능하다.

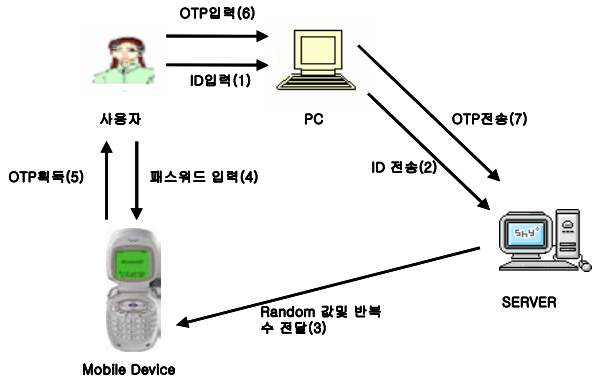



그림 3 . 인증 프로토콜

3.3 구현로직

1)개발환경

- OS : WINDOW2000 PROFESSIONAL
- PROGRAM LANGUAGE : JAVA JDK1.4.2
- SCRIPT LANGUAGE : JSP 1.2
- WEB-SERVER : TOMCAT 5.1
- MD4,MD5 해쉬함수
- EDITOR : JDEVELOPER

2) 소스코드

- web page
  login.html : ID입력페이지
  login_pass.html : 생성된 OTP입력페이지
  server.jsp : 입력받은 아이디를 체크하고, 랜덤값과 반복수를 에뮬레이터로 전달하고 마지막에 입력된 OTP를 계산하여 사용자 인증을 하는 파일.

- bean
  ServerMobile.java : 에뮬레이터에 메시지를 넘겨주는 역할의 파일

- Gui
  Emulator.java : 휴대폰을 구현한 파일

- 암호모듈
  MD.class : md4,md5가 상속받는 클래스
  MD4.class : md4 해쉬함수를 구현한 클래스
  MD5.class : md5 해쉬함수를 구현한 클래스
  OTP.class : OTP를 구현한 클래스

3) 프로그램 설계

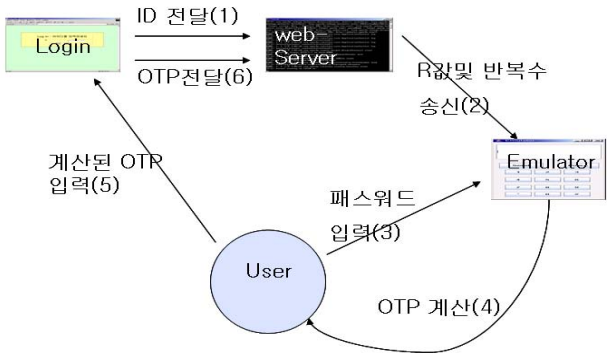
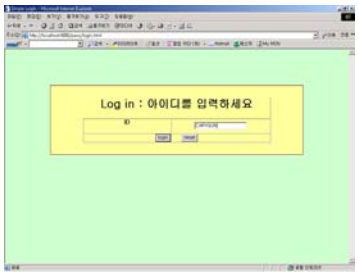


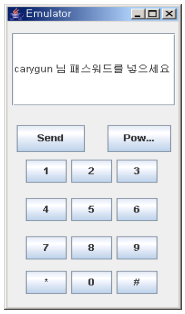

그림 4. 설계 흐름도

4) 구현내용

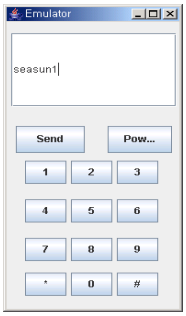



(1)ID 입력(login.html)

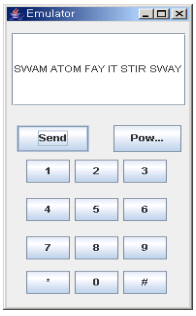
(2)server.jsp에서 처리후 R값과 반복수를 Emulator로넘김



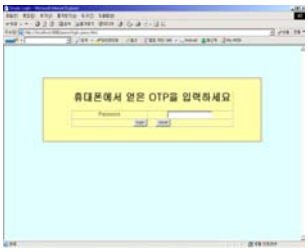

(3)sms메시지수신



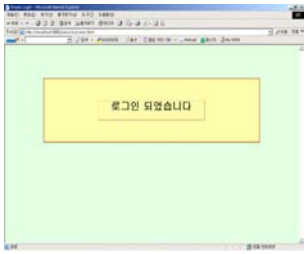

(4)password입력




(5)계산된 OTP값




(6)결과값을 패스워드로 입력




(7)확인후 로그인

그림 5 동작방식

3.4 제안 시스템의 보안성

1)도청에 의한 재생공격 방지 : 일회용 패스워드의 속성상 매번 새로운 패스워드가 생성되므로 재공격을 방지 가능하다.

2)이동장치 소유자만이 인증 : 휴대폰을 소유한 사람만이 로그인을 위한 SMS를 수신 가능하다. 하지만 이와 같은 환경에서는 휴대폰의 분실을 고려해야만 한다. 만약 사용자가 휴대폰을 분실하는 경우에도 OTP를 생성하기 위한 패스워드는 그 사용자만이 알고 있으므로,휴대폰을 습득한 사람일지라도 도용하기가 어렵다.

4)제안된 오프라인 사전공격 : 만약 이전의 OTP를 도청하고, 휴대폰을 훔친 공격자로부터의 오프라인 사전공격에 취약할 수 있다.

5)악의적 컴퓨터로부터의 비밀정보 보호 : 사용자가 사용하고 있는 컴퓨터가 악의적일 지라도, 사용자는 로그인시에 사용하는 OTP 계산을 위해서 휴대폰을 사용하기 때문에 사용자의 비밀정보인 패스워드를 노출하지 않는다.

본 논문의 제안 시스템은 서버가 사용자를 인증하는 단방향인증이다. 만약 상호인증이 필요한 경우, HTTP를 사용하는 웹 환경에서는 서버 인증만을 수행하는 SSL Protocol을 수행하여 사용자의 서버 인증을 부가적으로 수행 가능하며, 이러한 것은 단순한 아이디/패스워드 노출을 방지하기 위하여 SSL을 사용하는 것과는 차별적이다.

## 4.결론

본 논문에서의 설계되고 구현된 시스템은 고전적인 일회용 패스워드 기법과 SMS를 통하여, 안전한 사용자 인증을 수행 가능하다. 또한, 제안 시스템을 통하여 사용자는 휴대폰을 사용하여 언제 어느 지역에서나 성공적으로 안전하게 로그인을 수행할 수 있다.

## 5.참고문헌

[1]N. Haller, "The S/KEY One-Time Password System" , Proceedings of the ISOC Symposium on Network and Distributed System Security, February 1994, San Diego, CA

[2]박중길, 김영진, 김영길, 백규태, 백기영, 류재철 "S/Key를 개선한 일회용 패스워드 매커니즘 개발"

[3]이상근,방효장, "CDMA 무선기술",pp189-215,2000

[4]Jay spalan and Mike Burke, "Cellular Data Service Architecture and Signaling , IEEE Personal Communications" pp44-55,1994

[5]Vipul Goyal, How To Re-initialize a Hash Chain, http://eprint.iarc.org , 2004

[6]Min Wu , Simson Garfinkel, Rob Miller "Secure Web Authentication with Mobile Phones"

[7]삼성전자㈜, SCOS 1.5 Reference Manual, 1998.

[8]Jess Garms, Daniel Somerfield "Java Security" 2001