한국컴퓨터정보학회 동계학술대회 논문집 제22권 제1호 (2014. 1)

OTP를 이용한 사용자 계정 로그인 정보 관리 시스템 구현

정현희°, 신동렬*
°성균관대학교 정보통신대학 전자전기컴퓨터공학부
*성균관대학교 정보통신대학 전자전기컴퓨터공학부
e-mail: gusgml7041@naver.com°,drshin@ece.skku.ac.k*

Implementation of User Account Log-in Data Management System using OTP

Hyunhee JungO, Dong-Ryeol Shin*
°Dept. of Information and Communication Engineering, Sungkyunkwan Univ.
*Dept. of Information and Communication Engineering, Sungkyunkwan Univ.

● 요 약 ●

본 논문에서는 OTP를 이용한 사용자 계정 로그인 정보 관리 시스템 구현을 제안한다. 웹에서 패스워드(PW)를 통해 인증을 하는 대부분의 사용자는 편리를 위해 단순한 패스워드를 설정한다. 하지만 단순한 패스워드는 추측 공격 등 해킹 당할 위험이 높다. 그러므로 제시하고자 하는 시스템은 로그인 정보 중 ID와 PW를 복잡하게 설정하고 체계적으로 관리하여 보안성과 편리성을 동시에 높이고자 한다. 또한 PW를 통한 인증 방법의 단점인 추측 공격과 스나이퍼 공격의 취약점을 보완하기 위해 OTP(One-time Password) 기술을 이용하여 보안을 강화하고자 한다.

키워드: Password, OTP(One-time Password), Android

I. 서 론

현재, 전 세계적으로 스마트폰이 단기간에 급속한 성장세를 보이며 사회 전반으로 빠르게 확산됨에 따라 스마트폰 이용률이 아이들부터 어른들까지 다양한 연령대로 급속하게 증가하고 있다. 또한 스마트폰의 이용 계기는 1위로 '다양한 응용 소프트웨어를 이용하고 싶어서(67.1%)'인 것으로 나타났으며, 2위는 '수시로 인터넷을 이용하고 싶어서(56.8%)'이용하기 시작한 것이라고 조사되었다.[1]

이렇듯 많은 사람들이 애용하고 있는 스마트폰 상에서 웹사이트 또는 웹 어플리케이션의 서비스를 제공 받기 위해 사용자 계정을 만들어 로그인(Log-in)을 이용한다. 대부분의 사용자 계정 정보는 ID와 PW를 사용한다. 하지만 PW 인증 방식은 사용자들의 편리함을 위해 단순하거나 보안에 취약한 PW를 설정한다. 만약 보안에 취약함 암호를 설정할 경우, 추측될 수 있으며, 이를 통해 악의적인 공격자가 정당한 사용자로 위장하여 사용자의 개인정보가 침해되는 커다란 문제점이 나타날 수 있다.[2] 그래서 이러한 문제점을 해결하기 위해 PW의 복잡도를 높이거나, 주기적으로 변경하고자 한다. 하지만 PW의 복잡도를 높이거나, 또한 여러 곳에서 각각 다른 계정을 사용한다면 사용자의 PW의 관리 또한 더욱 어렵게 될 것이다.

따라서 본 논문에서는 이러한 단점을 극복하기 위해 ID/PW를 관리하는 시스템을 구현하며, 계정 로그인 정보를 안전하게 관리하기 위해 일회용 패스워드(OTP, One Time Password) 기술을 적용한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 제안하고자 하는 시스템의 주요 보안 기술인 OTP(One Time Password)에 대한 개요를 제시한다. 3장에서는 본 논문에서 제안하는 사용자 계정 로그인 정보 관리 시스템을 구체적으로 서술하고, 제안하고자 하는 시스템의 구현 및 결과에 대해 서술한다. 4장에서는 결론을 맺고 향후 연구에 관해 언급한다.

II. 관련 연구

1. OTP 기술

OTP(일회용 패스워드, One Time Password)란 OTP 토큰과 인증 서버 간 시간이나 seed와 같은 비밀 정보를 공유하고 이러한 정보를 해시 함수와 같은 알고리즘을 통해 생성된 값을 정해진 시간에 일회용 패스워드로 이용하는 사용자 인증 기법이다.[3] 이는 그 다음 사용될 일회용 비밀번호를 유추하는 것이 어려운 비밀번호 생성 기법을 사용한다. 이 기술은 일정 시간마다 전용 단말기 등에 새로운 비밀번호가 생성되어 시스템에 접근할 때마다 새로운 비밀번호를 입력해야하기 때문에 해킹이나 사용자의 관리 소홀 등으로 비밀번호가 노출되는 것을 방지할 수 있다. 만약 사용자 일회용 비밀번호가 노출되더라도 새로 생성된 비밀번호를 입력해야하기 때문에 훨씬 강력한 보안성을 제공한다.

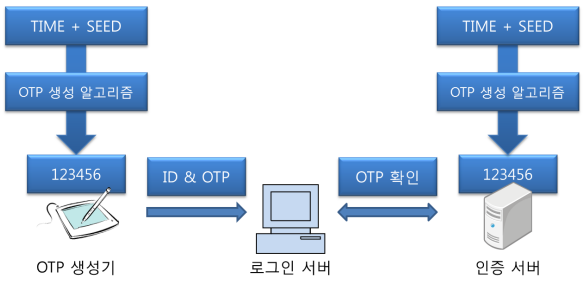

그림 1. OTP 인증 과정
Fig. 1. OTP Authentication Sequence

2. OTP 생성 및 인증 방식

OTP를 생성하는 방식에는 기본적으로 질의응답 방식, 시간 동기화 방식, 이벤트 동기화 방식으로 나누어져 있다.[3,4]

2.1 질의응답 방식

서버에서 난수 생성 등을 통해 임의의 수를 생성하고 클라이언트에 그 값을 전송하면, 클라이언트가 그 값으로 OTP를 생성해 응답한 값으로 인증하는 방식이다. 이 방식은 입력 값이 매번 임의의 값이 된다는 측면에서는 안전하지만, 서버와 클라이언트 사이의 통신 횟수가 비교적 많이 요구되어 중간에 가로채기 공격의 위험이 있다.

2.2 시간 동기화 방식

OTP를 생성하기 위해 사용하는 값으로 시간을 이용하는 방식이다. 클라이언트가 현재 시간으로 OTP를 생성해 서버로 전송하고, 서버는 같은 시간에 같은 방식으로 OTP를 생성하여 클라이언트가 전송한 값을 검사하여 인증한다. 이는 다른 OTP 생성 방식에 비해 안전하지만, 클라이언트와 서버 간의 시간 동기화가 정확하지 않으면 인증에 실패하게 된다는 단점이 있으며, 이를 보완하기 위해 일반적으로 1~2분 정도를 OTP 생성 간격으로 둔다.

2.3 이벤트 동기화 방식

서버와 클라이언트가 카운트 값을 동일하게 증가시키면서, 해당 카운트 값을 이용하여 OTP를 생성하여 인증하는 방식이다. 단, 클라이언트에서 OTP를 생성한 후 인증에 사용하지 않으면, 클라이언트와 서버 간의 카운트 값이 일치하지 않아 인증에 문제점이 있다. 이러한 문제점을 보완하기 위해 오차 범위를 두고 인증을 허용하거나, 카운트 값을 초기화 하는 방법 등이 사용된다.

III. 본 론

본 논문에서는 OTP 기술을 이용하여 사용자 계정 로그인 정보를 안전하게 관리하여 사용자의 개인정보 보호와 편리함을 제공하는 것을 목적으로 한다. 본 장은 사용자의 계정 로그인 정보를 관리하는 시스템에 대해 구체적으로 서술한 후, 구현 및 결과에 대해 서술한다.

1. 사용자 계정 로그인 정보 관리 시스템

제시하고자 하는 시스템은 사용자 인증 모듈, OTP 모듈, 로그인 정보 저장 모듈, 자동 로그인 모듈로 구성된다.

1.1 사용자 인증 모듈

사용자 인증 모듈은 시스템을 이용하기 위해 인증 과정을 거쳐야 한다. 처음 이용하는 사용자의 경우, 마스터 패스워드를 설정하고, OTP 모듈을 설치 및 설정해야 한다. 설정이 완료된다면, 이 모듈은 시스템을 이용하기 전에 마스터 패스워드와 OTP 모듈에서 생성한 일회용 패스워드를 입력해야 서비스를 진행 할 수 있다.

1.2 OTP 모듈

OTP 모듈은 사용자가 서비스 이용을 위해 시간 동기화 방식을 통해 인증 과정에서 필요한 일회용 패스워드를 생성한다. 이 모듈은 서비스 최초 사용 시, 난수인 일련번호를 생성한다. 사용자는 이 일련번호를 시스템에 입력하면, OTP 모듈과 시스템은 시드를 공유하여 일회용 패스워드를 생성한다.

OTP를 이용한 인증 과정은 다음과 같다. OTP 모듈은 최초 이용 시, 일련번호를 생성하고, 시스템과 공유한다. 공유한 일련번호를 seed값으로 이용하며, 이 seed 값과 로그인 요청 시각을 이용하여 공유한 해시 알고리즘을 통해 OTP 값을 생성한다. 이를 시스템에 마스터 패스워드와 함께 입력한다. 이를 받은 시스템은 공유한 seed 값, 로그인 요청 시각과 해시 알고리즘을 이용하여 계산하고 검증한다. 검증이 완료되면 사용자는 서비스를 이용 할 수 있다.

1.3 로그인 정보 저장 모듈

로그인 정보 저장 모듈은 사용자의 계정 로그인 정보를 시스템에 저장한다. 저장될 데이터는 AES-128 암호화 알고리즘을 통해 저장된다. 사용자는 ID, PW를 입력하고, 추가적으로 사용하고자 하는 웹사이트 혹은 웹 어플리케이션을 선택해야한다. 선택된 항목은 자동 로그인 모듈에서 활용한다.

1.4 자동 로그인 모듈

자동 로그인 모듈은 사용자가 저장한 로그인 정보를 이용하여 이용하고자 하는 웹 사이트나 웹 어플리케이션에 클립보드 기능을 통해 자동 입력 및 로그인하는 모듈이다. 이 모듈은 사용자의 개인정보 유출 가능성을 없애기 위해 실행 후, 클립보드에 남겨진 정보를 삭제한다.

2. 구현 및 결과

본 논문에서 제시하고자 하는 시스템의 개발 환경은 다음과 같다. [표 1]에서 제시한 개발환경 상에서 JAVA 프로그래밍을 하였다.[5]

표 1. 시스템 개발 환경
Table 1. System Development Environment

항목	내용
OS	Windows 7
Tools	Eclipse, Android SDK
Programming Language	JAVA
Target Device	SHV-E330S

본 시스템은 그림 2와 같은 순서로 구동한다. 프로그램 실행 시, 사용자 인증 모듈에 진입한다. 이 모듈에서 Master PW와 OTP 모듈을 통해 받은 OTP 값을 입력하면 로그인 정보 저장 모듈을 통해 로그인 정보를 안전하게 저장할 수 있고, 이후 자동 로그인 모듈을 통해 알맞은 웹 사이트나 웹 어플리케이션에 로그인 할 수 있다.

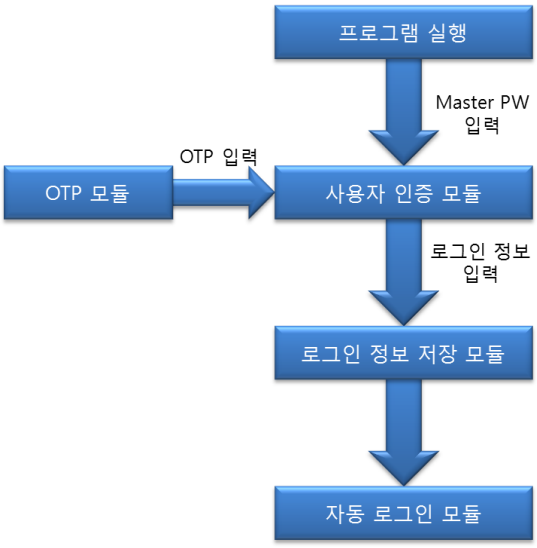

그림 2. 프로그램 실행 과정
Fig. 2. Program Execution Sequence

다음 그림 3는 프로그램 구동 시 사용자 인증 모듈이 실행된 화면이다. 이 화면에서 사용자가 인증 받는다면 로그인 정보를 저장 할 수 있는 모듈로 이동할 수 있다.

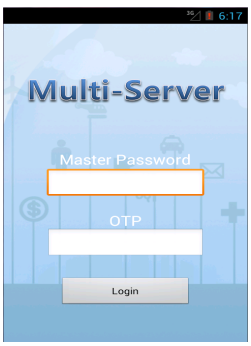

그림 3. 프로그램 실행화면
Fig. 3. Program Execution Screen

Ⅳ. 결 론

본 연구에서는 OTP 기술을 이용하여 사용자의 계정 로그인 정보를 효율적으로 관리하는 시스템을 개발하는 것을 목표로 하였다. 연구 결과는 OTP 기술을 이용함으로써 사용자의 개인정보를 보호할 수 있다. 또한 인증된 사용자라면 자동 로그인 모듈을 이용하여 간단한 방법으로 인증할 수 있다.

하지만 자동 로그인 모듈은 특정한 웹 사이트나 웹 어플리케이션에만 동작이 가능하다는 문제점이 있다. 따라서 향후 자동 로그인 알고리즘을 연구하여 보다 완성도 높은 소프트웨어 모듈을 개발하는 것이 앞으로의 과제로 남아있다.

참고문헌

[1] J.Y. Eim, J.Y. Yoo, et al., "2012's State Survey using Smartphones", The Korea Communications Commission and The Korea Internet & Security Agency, pp. 10, December 2012.

[2] J.Y. Eim, J.Y. Yoo, et al., "Guidelines for Information Security Management System Control Information", The Korea Information Security Agency, pp. 79-81, December 2012.

[3] D.H Choi, S.J Kim, D.H Woo, "Technology Analysis and Standardization Trend of OTP". Journal of The Korea Institute of Information Security, Vol. 17, No. 3, pp. 12-17, June. 2007.

[4] Wikipedia One-time Password, *http://ko.wikipedia. org/ wiki/ OTP_(%EB%B2%88%ED%98%B8)*

[5] Android Developers, http://developer.android.com