

PassWorld

Team 5

김선준, 유진영, 조정민

Dept. Electronics and Computer Engineering
Chonnam National University
Gwangju

Function and Work distribution

I. MOTIVATION

비밀번호는 인터넷을 사용하는 데 필수적인 요소입니다. 인터넷 상에서 본인임을 증명하는 첫 번째 수단이고, 개인정보를 보호해주는 파수꾼의 역할도 합니다. 이런 중요성 때문에 많은 웹사이트가 이용자들에게 대/소문자 혼합사용, 일정길이 이상, 특수문자 사용과 같은 조건을 만족하는 비밀번호를 설정하도록 요구합니다. 문제는 사이트마다 요구하는 비밀번호의 형식이 제각각이고, 주기적인 변경을 요구한다는 것입니다. 이 때문에 사용자는 로그인할 때 비밀번호를 기억해내지 못하는 소위 '패스워드 증후군'에 빠지게 됩니다.

위와 같은 문제를 해결하기 위해 웹 브라우저 자체적으로 혹은 확장프로그램을 통하여 비밀번호를 저장하는 방식의 프로그램들이 이미 사용되고 있습니다. 하지만 이러한 프로그램들은 사용자를 자신의 비밀번호에 대해 무관심하게 만듭니다. 또한, 로그인에만 반응하게 되어있는 경우가 많아서 로그인 화면 외의 페이지에서 비밀번호를 요구할 때 반응하지 않아 곤란한 경우가 발생하기도 합니다.

이 프로그램은 비밀번호를 자주 잊어버리는 사람들을 위해 기획되었습니다. 이 프로그램은 사용자들이 자신의 비밀번호를 체계적으로 관리할 수 있게 도와줍니다. 또한, 사용자가 안전한 비밀번호를 생성할 수 있도록 프로그램 내에서 가이드라인을 제공하여 도와주고, 한 단계 더 나아가 사용자에게 비밀번호에 관한 관심을 지속적으로 환기해 줌으로써 사용자가 안전한 인터넷 생활을 할 수 있도록 도울 것입니다.

II. CHARACTERISTICS

이 프로그램의 특징은 사용자의 비밀번호를 저장하고 관리하면서 자동입력, 로그인 기능을 제공하여 사용자의 편의성에만 초점을 맞추고 개발된 기존 프로그램들과는 다르게, 사용자가 프로그램에 비밀번호를 저장한다는 점을 고려하여, 비밀번호를 주소록 형식으로 볼 수 있게 해서 사용자가 비밀번호를 체계적으로 관리할 수 있도록 도와주는 역할을 합니다. 사용자는 자신이 등록한 키워드로 검색해서 자신의 비밀번호를 언제든지 열람할 수 있습니다. 또한, 등록된 비밀번호들의 교체시기를 알려주고, 안전한 비밀번호를 만들 수 있도록 가이드를 제공합니다. 그리고 비밀번호를 ARIA알고리즘을 이용해 암호화한 다음 사용자의 로컬디스크에 있는 DB에 데이터를 저장해서 비밀번호를 서버에 저장하는 경우 발생할 수 있는 보안 사고로 인해 개인정보가 유출될 수 있는 위험을 예방하였습니다.

A. Related applications

Describe the characteristics of previous related applications. 관련 어플리케이션의 특징에 대하여 설명합니다.

- 알패스, LastPass : 웹브라우저에서 툴바의 형태로 설치되는 프로그램으로, 사용자가 로그인 정보를 등록하면 자동입력/자동로그인을 해준다. 로그인 정보를 서버에 보내 저장하여, 다른 컴퓨터에서 접속할 때에도,

프로그램을 설치하여 로그인 하면 자신의 로그인 정보를 가져와서 사용할 수 있다.

-웹브라우저 내장 비밀번호 저장기능 : 웹브라우저에 내장된 기능으로 사용자가 직접 등록하거나, 로그인 과정을 감지할 경우 사용자에게 물어보고 입력된 정보를 저장한 후 필요시 ID/비밀번호를 자동입력 또는 자동로그인을 해준다.

B. Characteristics of the target application

대상 어플리케이션의 특징

Describe the characteristics of the target application. Then, compare the characteristics of the target application to the previous ones. 대상 어플리케이션의 특징을 설명하고, 관련된 어플들과의 차이를 비교합니다.

-알패스와 LastPass는 웹브라우저에 툴바를 설치하여 사용합니다. 사용자의 로그인 정보를 저장하여, 사용자가 로그인 정보를 저장해둔 웹페이지에 접속하면 자동으로 로그인 해줍니다. 하지만 프로그램에 저장되어 있는 비밀번호를 알 수 없기 때문에 주기적인 비밀번호 교체에 장애요인이 됩니다. 이를 해결하기 위해 사용자가 자신이 등록한 비밀번호를 찾아볼 수 있도록 하였습니다. 또한 기존의 프로그램들은 다른 컴퓨터에서 사용할 수 있도록 서버에 로그인 정보를 저장하는 방식을 사용하기 때문에 그 프로그램의 서버가 해커들의 표적 될 수 있어 보안상의 위험이 존재합니다. 이를 해결하기 위해 PassWorld에서는 서버로 전송하지 않고 로그인에 필요한 정보들을 사용자의 로컬 디스크 내에 암호화하여 저장하도록 했습니다.

-웹브라우저 내장 비밀번호 저장기능은 경우에 따라 웹페이지에서 로그인 혹은 비밀번호를 요구한다는 것을 인식하지 못하는 문제가 발생합니다. PassWorld는 사용자의 비밀번호를 저장하였다가 사용자가 필요로 할 때 검색을 통하여 찾아볼 수 있도록해서 이러한 문제를 해결하였습니다.

-사용자가 비밀번호를 사용한 횟수를 기록하여 검색을 했을 때 가장 많이 사용한 순서대로 정렬하여 사용 편의성을 높였습니다. 그리고 사용자의 필요에 따라 검색한 결과의 비밀번호 부분을 가릴 수 있도록 하였고, 60일 이상이 지난 비밀번호의 경우 날짜를 적색으로 강조하여 교체시기가 되었음을 알 수 있도록 하였습니다.

III. FUNCTION SPECIFICATION

로그인/등록	로그인	Google 에서 제공하는 GoogleAuthenticator 를 이용하여 TOTP(Time-based One Time Password)방식으로 로그인합니다. 사용자는 휴대기기의 어플리케이션 'Google Authenticator'에서 생성되는 otp 코드를 로그인창에 입력하여 로그인할 수 있습니다.
	등록	사용자의 이름, 이메일을 이용하여 OTP 코드 생성에 사용하는 Secret code 를 생성하고 DB 에 저장합니다. Secret code 를 사용자에게 기기에 입력하는 과정의 편의성을 고려하여 QR 코드를 통해서도 등록할 수 있게 하였습니다. 생성된 Secret code 사용자의 이름과 함께 DB 안에 암호화되어 저장됩니다. 내부 데이터의 보호를 위해 사용자가 OTP 를 재등록 하게되면 기존에 저장되어있는 모든 데이터들이 삭제됩니다.
홈	검색	사이트 이름, 키워드를 입력하고 검색버튼을 누르면 검색창 하단의 표에 결과를 출력합니다. 정확한 검색어를 입력하지 않고 일부만 입력하더라도 검색이 가능합니다. 검색된 결과는 비밀번호를 사용한 횟수로 정렬됩니다.
	비밀번호 변경 알림	검색 결과 중 최근 수정일자로부터 60 일 이상 지났을 경우 수정일자가 붉은색으로 강조됩니다.
	비밀번호 클릭해서 복사	검색결과에서 항목의 행을 더블클릭하면 그 항목의 비밀번호를 사용자의 클립보드에 복사합니다.
	비밀번호 masking	검색버튼 옆의 체크박스에 체크를 하면 비밀번호 열을 마스킹해서 비밀번호 노출을

		막을 수 있습니다.
비밀번호 관리	비밀번호 등록	사이트의 이름, 검색에 사용할 키워드, 사용자의 ID, 사용자의 비밀번호, 생성일자를 입력하여 DB 에 계정 정보를 등록합니다. 사이트의 이름과 ID, 비밀번호는 필수 입력항목이며, 사이트의 이름과 ID 두 가지가 같은 항목이 DB 에 존재할 경우 등록을 막아 데이터의 중복 등록을 방지합니다. 생성일자는 사용자가 임의로 지정할 수 있으며, 미입력시 자동으로 현재날짜가 저장됩니다. 비밀번호 오입력을 방지하기 위해 비밀번호를 2 번 입력하도록 하였고, 입력된 비밀번호에 대해 안전성 검사를 진행하여 결과를 보여줍니다.
	비밀번호 수정	검색결과에서 체크한 항목의 데이터를 불러온 후 수정하게 됩니다. 등록기능과 동일하게 비밀번호 안전성검사 및 동일 비밀번호 등록 알림 기능이 적용되어 있습니다.
	비밀번호 삭제	검색결과에서 체크한 항목들을 삭제합니다. 수정기능과는 다르게 2 개이상 체크하여 한번에 삭제할 수 있습니다.
	비밀번호 안전성 검사	비밀번호를 입력할 때 비밀번호의 길이, 포함된 문자의 종류, 이미 사용되고 있는 비밀번호인지를 고려하여 안전성을 테스트하고 사용자에게 결과를 보여줍니다.
	비밀번호 사용횟수	비밀번호를 클릭하여 복사할 때 DB 에 count 를 저장하여 복사한 횟수를 저장합니다. 이 정보를 바탕으로 사용자가 비밀번호를 검색할 때 자주 사용한 계정 정보 순서대로 정렬됩니다.

IV. REQUIREMENT LISTS

- ① 사용자가 등록하는 비밀번호를 DB 를 통하여 관리할 수 있어야한다.
- ② 사용자가 등록한 비밀번호를 포함한 중요한 항목들은 암호화한 후 저장되어야 한다.
- ③ DB 에 등록되어 있는 비밀번호를 수정/삭제 할 수 있어야한다.
- ④ 프로그램에 로그인할 때 사용자가 비밀번호를 기억하고 있을 필요가 없어야 한다. (Google OTP 이용)
- ⑤ 사용자가 OTP 를 등록할 때 OTP 와 OTP 생성 어플리케이션 (Google Authenticator)의 사용 방법을 알려줘야한다.
- ⑥ 사이트 이름 뿐만 아니라 사이트 이름의 일부분 또는 사용자가 등록한 키워드로도 검색 할 수 있어야한다.
- ⑦ 검색 결과 리스트에서 등록된 비밀번호를 클릭해서 바로 복사할 수 있어야 한다.
- ⑧ 검색결과 리스트에서 변경 주기가 임박한 비밀번호를 사용자에게 알려준다.
- ⑨ 사용자가 등록하려고 하는 비밀번호의 안전성을 검증해주고, 이미 다른 사이트에서 사용 중인 비밀번호일 경우 알려준다.

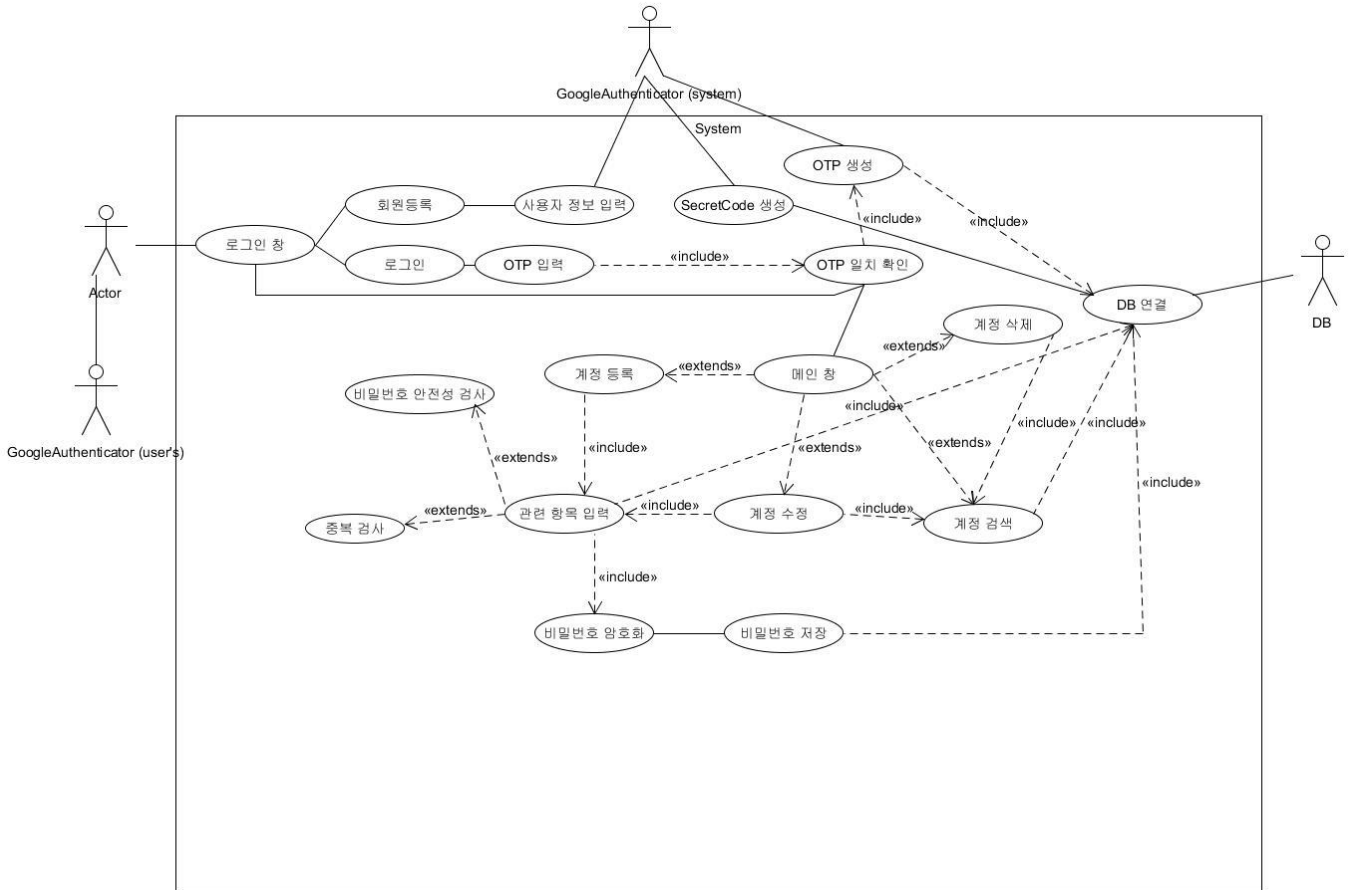
V. USECASES

- 회원가입 및 로그인
 - OTP 등록
 - i. 로그인 창에서 회원등록 버튼을 클릭한다.
 - ii. 회원등록 창이 출력된다.
 - iii. 사용자 이름과 이메일을 입력하고 등록을 누르면 'Google Authenticator'에 등록할 수 있는 secret code 를 생성하고 QR 코드를 팝업으로 띄워준다.

- iv. 정보 입력란 아래에는 'Google Authenticator'의 사용방법을 설명해주는 글을 첨부한다.
 - v. 등록 버튼을 누르면 프로그램 내에서 OTP 코드를 생성할 때 필요로 하는 secret code 와 사용자 이름을 DB 에 암호화 하여 저장한다.
 - vi. 정상적으로 저장되었으면 로그인 화면으로 돌아온다.
- 로그인
 - i. 로그인 창에 사용자의 휴대기기의 'Google Authenticator'에 표시되는 OTP 코드를 입력하고, 로그인 버튼을 누른다.
 - ii. 입력한 OTP 코드와 프로그램 내에서 생성된 OTP 코드를 비교한다.
 1. 일치하지 않거나 제대로 입력하지 않았을 경우 에러 메시지를 출력하고 확인을 누르면 로그인 창으로 돌아간다.
 - iii. 값이 일치할 경우, 메인 창을 출력한다.
 - 메인화면
 - 비밀번호 검색
 - i. 메인화면의 검색칸에 검색할 키워드를 입력하고 옆에 있는 검색버튼을 누른다.
 1. DB 에서 입력한 문자를 포함하는 키워드들을 검색한다.
 2. 검색칸 옆에 있는 체크 박스에 체크를 하면, 검색 결과들의 비밀번호가 마스킹된다.
 - ii. 메인화면의 목록에 검색된 결과들을 사용 빈도순으로 출력한다.
 1. 목록에는 체크박스, 사이트 이름, 키워드, ID, 비밀번호, 비밀번호 등록일이 포함된다.
 - A. 만료기간이 특정 기간 이하로 남았을 경우, 등록일의 글자가 적색으로 강조된다.
 - B. 리스트에서 표시되는 정보들을 더블 클릭하면 해당되는 비밀번호가 복사된다.
 - 비밀번호 등록
 - i. 메인화면 하단에 있는 등록 버튼을 누른다.
 - ii. 비밀번호 등록 창이 출력된다.
 - iii. 등록창에 있는 항목들에 각각 사이트 이름, 키워드, 아이디, 비밀번호, 비밀번호 등록일을 입력한다.
 1. 비밀번호 입력란 아래에 비밀번호의 특수문자 포함여부, 길이 등의 정보를 종합하여 안전성을 평가한 결과를 보여준다.
 2. 비밀번호 입력란 아래 재입력란을 추가하고 '일치 여부' 버튼을 이용해서 잘못된 비밀번호가 등록되는 것을 방지하고, 기존에 등록된 비밀번호 중 중복되는 비밀번호가 있는지 검색한 결과를 보여줍니다.
 - iv. 입력을 완료하였으면 확인 버튼을 누르고, 작성을 취소하려면 취소 버튼을 누른다.
 1. 확인 버튼 클릭 시, DB 를 검색하여 동일한 사이트가 등록되어 있고 등록된 id 도 같은 경우 사용자에게 에러 메시지를 출력한다.
 2. 취소 버튼 클릭 시, 재확인 창을 출력한다.
 3. 등록된 정보들은 DB 에 암호화 되어 저장된다.
 - v. 정상적으로 저장되었으면 메인 창으로 돌아간다.
 - 비밀번호 수정
 - i. 리스트 되어있는 항목들 중 수정할 항목의 체크박스를 클릭하여 체크한다.

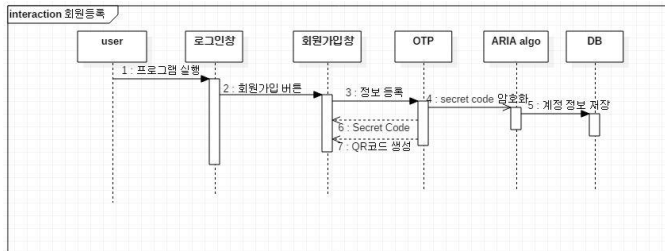
- ii. 메인화면 하단에 있는 수정 버튼을 누른다.
 1. 두개 이상 선택된 경우/아무것도 선택되지 않은 경우 에러 메시지 창을 출력한다.
 - iii. 사이트 정보를 등록할 때 등록한 정보들이 입력되어 있는 상태의 창을 출력한다.
 1. 비밀번호 입력란 옆에는 비밀번호의 특수문자 포함여부, 길이, 동일 비밀번호 존재여부를 종합하여 안전성을 평가해서 비밀번호 항목 아래에 결과를 보여줍니다.
 2. 비밀번호 입력란 아래 재입력란을 추가하고 ‘일치 여부’ 버튼을 이용해서 잘못된 비밀번호가 등록되는 것을 방지하고, 기존에 등록된 비밀번호 중 중복되는 비밀번호가 있는지 검색한 결과를 보여줍니다.
 - iv. 입력을 완료하였으면 확인 버튼을 누르고, 작성을 취소하려면 취소 버튼을 누른다.
 1. 확인 버튼 클릭 시, DB 를 검색하여 동일한 사이트가 등록되어 있고 등록된 id 도 같은 경우 사용자에게 오류메시지를 출력한다.
 2. 취소 버튼 클릭 시, 재확인 창을 출력한다.
 - v. 정상적으로 작업이 완료되면 메인 창으로 돌아간다.
- 비밀번호 삭제
- i. 리스트 되어있는 비밀번호들을 클릭하여 체크한다.(복수선택 가능)
 - ii. 메인화면 하단에 있는 삭제 버튼을 누른다.
 1. 복구가 불가능 하다는 경고문을 포함하는 재확인 창이 출력된다.
- 2. 재확인 창에서 확인을 누르면 선택된 항목들이 삭제된다.
- iii. 메인 화면으로 돌아간다.

VI. USECASE DIAGRAM

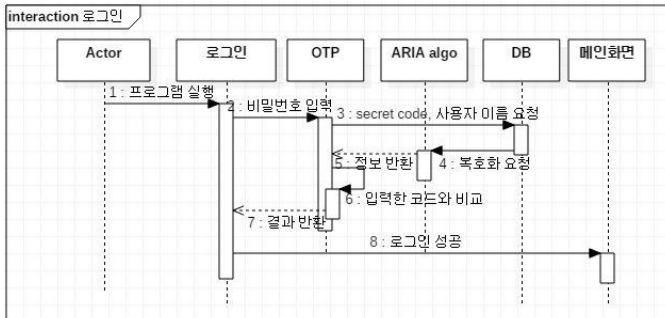


VII. SEQUENCE DIAGRAM

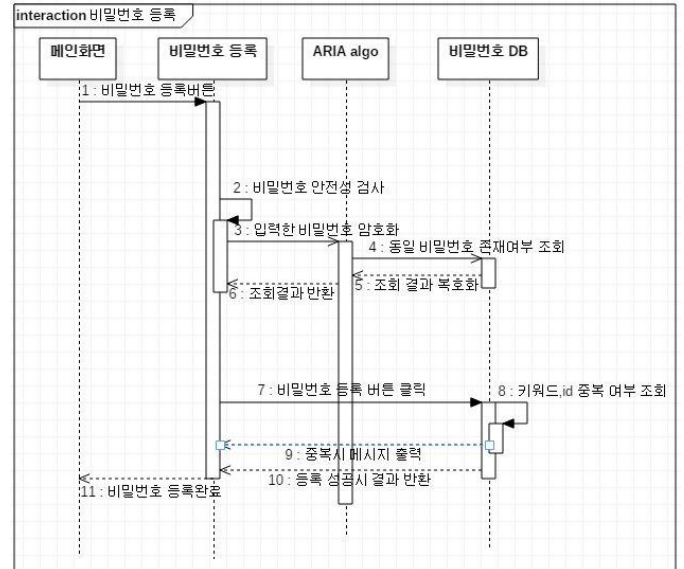
● 회원등록



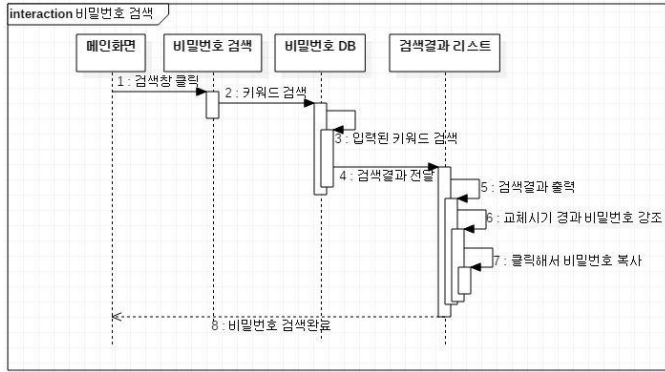
● 로그인



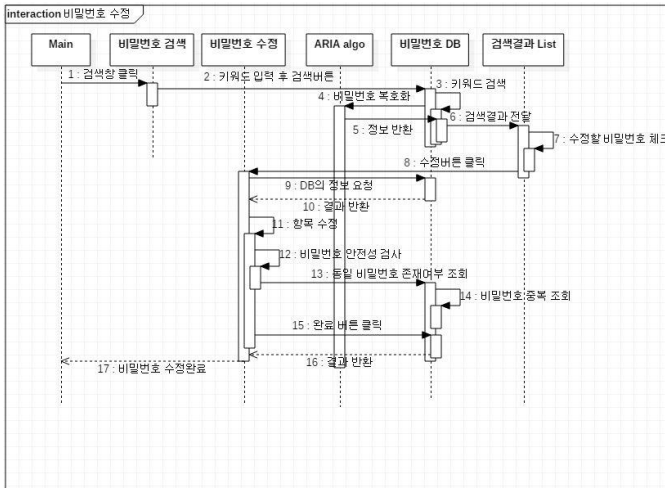
● 비밀번호 등록



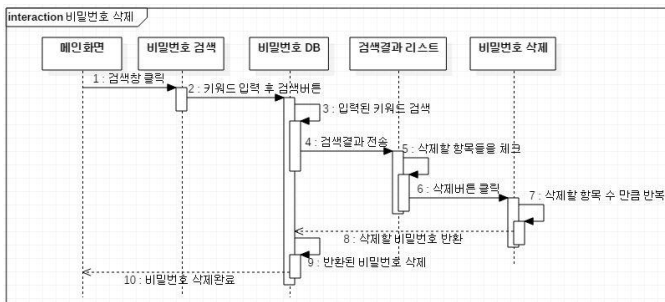
● 비밀번호 검색



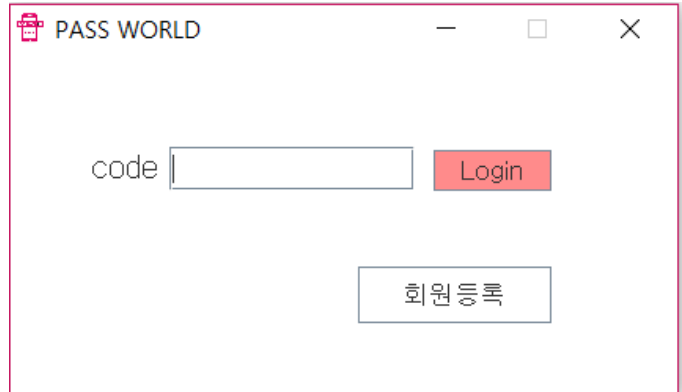
● 비밀번호 수정



● 비밀번호 삭제



● 로그인 화면



● 회원등록 화면



* Google Authenticator 사용법

1. 'Google Authenticator' 어플을 설치합니다.
2. 'PassWorld' 프로그램 화면에서 이름과 계정명을 입력하고 등록버튼을 누릅니다.
3. 어플에서 '+'버튼을 클릭합니다.
- 3-1. '바코드 스캔'을 눌러 화면의 QR코드를 찍습니다.
- 3-2. '직접 입력'을 눌러 'PassWorld' 프로그램 내에서 생성된 Secret Code를 직접 입력합니다.
4. 등록 후에는 'Google Authenticator' 어플에 계정명과 6자리의 숫자로 된 코드가 생성됩니다.

* 로그인 시, 'PassWorld' 프로그램의 로그인 화면에서 코드 입력 칸에 'Google Authenticator' 어플의 6자리의 숫자를 입력합니다.

* 회원 등록은 한 계정만 가능합니다. 재등록시, 기존의 OTP관련 데이터는 사라집니다.

● 메인화면

PASS WORLD

SEARCH

	사이트 이름	키워드	ID	PassWord	등록일자
<input checked="" type="checkbox"/>	네이버	naver	abc123	otpotp.88	2017-12-07
<input type="checkbox"/>	네이버	naver	def456	88.otpotp	2017-12-07
<input type="checkbox"/>	다음	daum	ghi789	.otpotp88	2017-12-07
<input type="checkbox"/>	다음	daum	aaa111	mola-+-	2017-12-07
<input type="checkbox"/>	구글	google	google1	google1234..	2017-12-07
<input type="checkbox"/>	구글	google	google2	google-+-	2017-12-07
<input type="checkbox"/>	박스	bugs	bugsbugs	musicismylife-*	2017-12-07
<input type="checkbox"/>	멜론	melon	melon1	watermelon!!	2017-12-07

등록 수정 삭제

● 계정 정보 등록/수정 화면

PASS WORLD

site 이름

Key Word

ID

암호

암호 재확인

일치여부

등록일자

확인 취소

● 기타 기능들

암호

위험 - 권장 비밀번호 길이는 8자리 이상입니다.

암호

경고 - 특수문자가 포함되지 않았습니다.

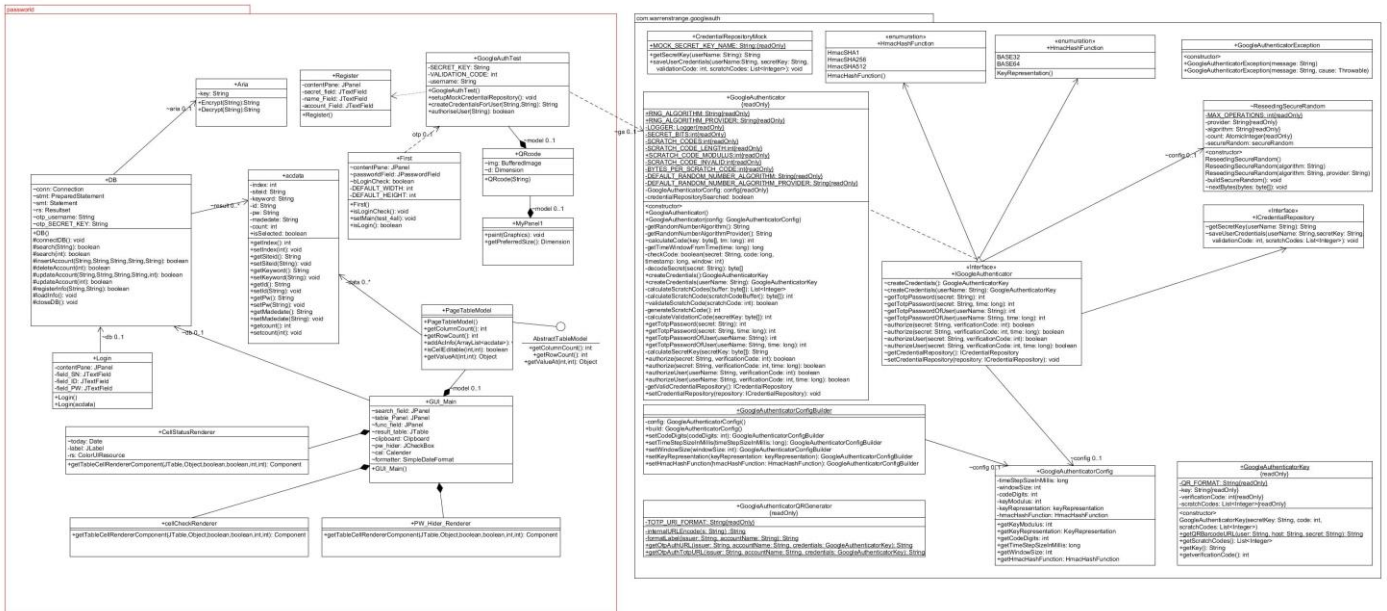
암호

안전 - 안전한 비밀번호입니다.

클릭하면 닫힘



IX. CLASS DIAGRAM



X. SCREENSHOT OF API MANUAL

PACKAGE CLASS USE TREE DEPRECATED INDEX HELP

PREV PACKAGE NEXT PACKAGE FRAMES NO FRAMES

Package passworld

Class Summary

Class	Description
acdata	the instance for storing user's account information
Aria	In cryptography, ARIA is a block cipher designed in 2003 by a large group of South Korea researchers.
DB	connect to ext/main.db schema of main.db's table 'Main' CREATE TABLE Main (siteid text not null collate nocase, //The name of the site can not be blank. and They are not case-sensitive.
First	
GoogleAuthTest	
GUI_Main	
Login	
QRcode	
Register	

PACKAGE CLASS USE TREE DEPRECATED INDEX HELP

PREV PACKAGE NEXT PACKAGE FRAMES NO FRAMES



XI. SCREEN SHOT OF APPLICATION DEMO

● 더블클릭하여 복사

	사이트 이름	키워드	ID	PassWord	등록일자
<input type="checkbox"/>	sadfasdf	asdfasdf	asdfasdf	1231231232	2017-12-07
<input type="checkbox"/>	sadfasdf	asdfasdf	asdfasdfaa	1231231232	2017-12-07
<input type="checkbox"/>	dsfa	asdfasdf	asdfasdf	111111qqqq	2017-12-07
<input type="checkbox"/>	dsfs	sdsds	asda	123123123	2017-12-07
<input type="checkbox"/>	qweqwe	qweqweqwe	qweqweqwe	123123123	2017-12-07

알림
1231231232 복사완료
확인

등록 수정 삭제

● 교체시기 경과 항목 글자색 변경

	사이트 이름	키워드	ID	PassWord	등록일자
<input type="checkbox"/>	sadfasdf	asdfasdf	asdfasdf	1231231232	2017-12-07
<input type="checkbox"/>	sadfasdf	asdfasdf	asdfasdfaa	1231231232	2017-12-07
<input type="checkbox"/>	네이버	test	test123	123123123!@#	2017-05-05

등록 수정 삭제

● 계정 등록

PASS WORLD

이름 TEST

계정명 daum@naver.com

등록

Secret code LVPYLXJISUE5SKDR

* Google Authenticator 사용법

1. 'Google Authenticator' 어플을 설치합니다.
2. 'PassWorld' 프로그램 화면에서 이름과 계정명을 입력하고 등록버튼을 누릅니다.
3. 어플에서 '+' 버튼을 클릭합니다.
- 3-1. '바코드 스캔'을 눌러 화면의 QR코드를 찍습니다.
- 3-2. '직접 입력'을 눌러 'PassWorld' 프로그램 내에서 생성된 Secret Code를 직접 입력합니다.
4. 등록 후에는 'Google Authenticator' 어플에 계정명과 6자리의 숫자로 된 코드가 생성됩니다.

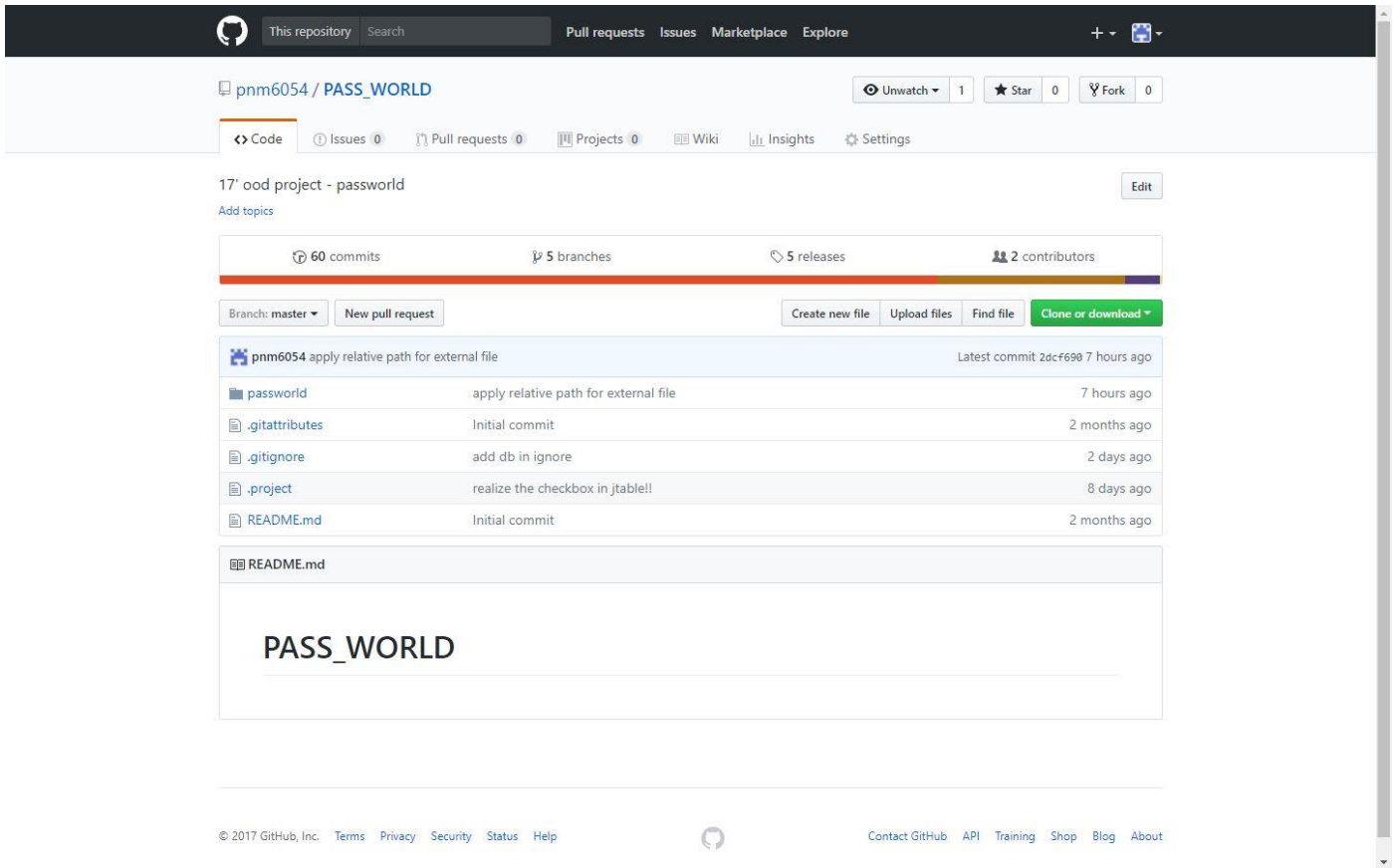
* 로그인 시, 'PassWorld' 프로그램의 로그인 화면에서 코드 입력 칸에 'Google Authenticator' 어플의 6자리의 숫자를 입력합니다.

* 회원 등록은 한 계정만 가능합니다. 재등록시, 기존의 OTP관련 데이터는 사라집니다.

● 비밀번호 마스크

	사이트 이름	키워드	ID	PassWord	등록일자
<input type="checkbox"/>	네이버	naver	def456	*****	2017-12-07
<input type="checkbox"/>	다음	daum	modify	*****	2017-12-07
<input type="checkbox"/>	다음	daum	aaa111	*****	2017-12-07
<input type="checkbox"/>	구글	google	google1	*****	2017-12-07
<input type="checkbox"/>	구글	google	google2	*****	2017-12-07
<input type="checkbox"/>	벅스	bugs	bugsbugs	*****	2017-12-07
<input type="checkbox"/>	멜론	melon	melon1	*****	2017-12-07

XII. SCREENSHOT OF GITHUB PAGES



XIII. WORK DISTRIVUTION

김선준	비밀번호 관리(DB) 791 Lines	Sqlite 를 이용하여 DB 를 구현하고, DB 에서 데이터를 입출력하는데 필요한 기능(ex. insert, update, delete, select)들과 비밀번호의 등록/수정/삭제에 필요한 기능을 맡았습니다. 비밀번호 안전성 검사, 중복된 비밀번호 존재여부 검색, 비밀번호 항목 중복 등록 방지, 비밀번호 항목의 암호화/복호화를 구현합니다. Main 화면을 구현했고, 비밀번호 마스킹, 교체필요 항목 글자색 변경, 더블 클릭하여 복사 등의 기능을 구현하였습니다.
유진영	회원등록/로그인(OTP) 254 Lines	Google Authenticator 를 이용한 회원 등록과 로그인 기능을 맡았습니다. 회원등록과정에서 발생하는 Secret Code 와 생성시간을 DB 의 계정 정보를 저장하는 테이블과는 별개의 테이블에 암호화 하여 저장하고,

		로그인 할 때는 저장된 Secret Code 와 user name 을 이용하여 프로그램 내부에서 OTP 코드를 생성하여 사용자가 입력한 코드와 비교합니다. 이를 통해 프로그램은 사용자가 입력한 OTP 를 검증하여 로그인을 승인할 수 있게 됩니다..
조정민	인터페이스 디자인(SWING) 511 Lines	프로그램의 전체적인 인터페이스 디자인을 맡았습니다. 로그인, 회원등록, 비밀번호 등록/수정창을 SWING 을 통하여 구현하고, 프로그램 사용시 발생하는 에러 메시지들과 조건문들을 구현하였습니다.