Sécurité et utilisabilité :
Le cas des mots de passe graphiques

TER/Projet proposé par M. PALANQUE Philippe. ICS Team. IRIT.

Réalisé par l'équipe MBPL

- JEANMOUGIN Pierre
- LACHERAY Benjamin
- LE QUERE Lilian
- MOUGEOT Matteo

M1 informatique 2015 - 2016

Structure de la présentation

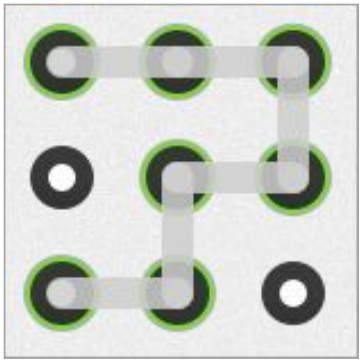
1. Présentation du TER
    a. Présentation du sujet
    b. Les types de méthodes d'authentification
    c. Les différentes vulnérabilités
    d. Les méthodes d'authentification
    e. Tableaux synthétiques
    f. Conclusion

2. Présentation du Projet
    a. Sujet du projet
    b. Notre réalisation
    c. Démarche, organisation
    d. Conception
    e. Conclusion et perspectives

TER.
Sécurité et utilisabilité :
Le cas des mots de passe graphiques

Présentation du sujet

- Sujet
- Méthodologie



Types de méthodes d’authentifications

- Reconnaissance (recognition)

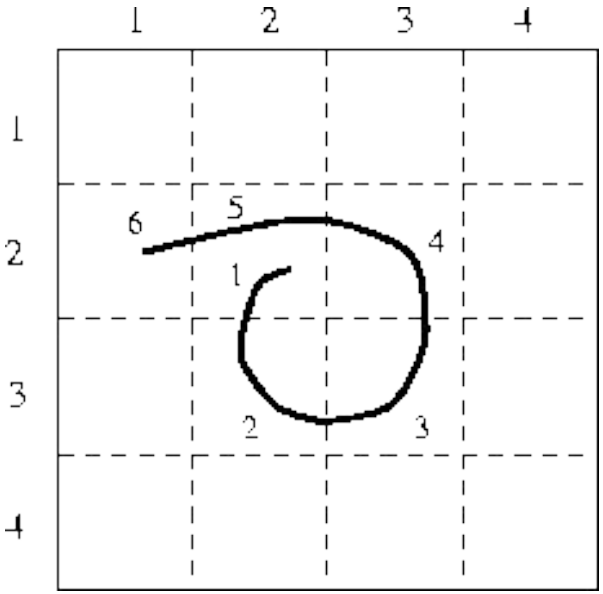
- Rappel pur (pure recall)
- Rappel indicé (cued recall)

- Hybrides

Les différentes vulnérabilités

- Dictionary attacks
- Shoulder surfing
- Brute force attacks
- Smudge attacks
- Eye tracking

Draw-A-Secret



Sécurité

+ Résistant au Shoulder Surfing (Decoy Strokes, Disappearing Strokes, Line Snaking)
+ RDAS > DAS Dictionnary et Smudge Attacks
- DAS sensible au Shoulder Surfing
- BDAS sensible aux Dictionary Attacks

Utilisabilité

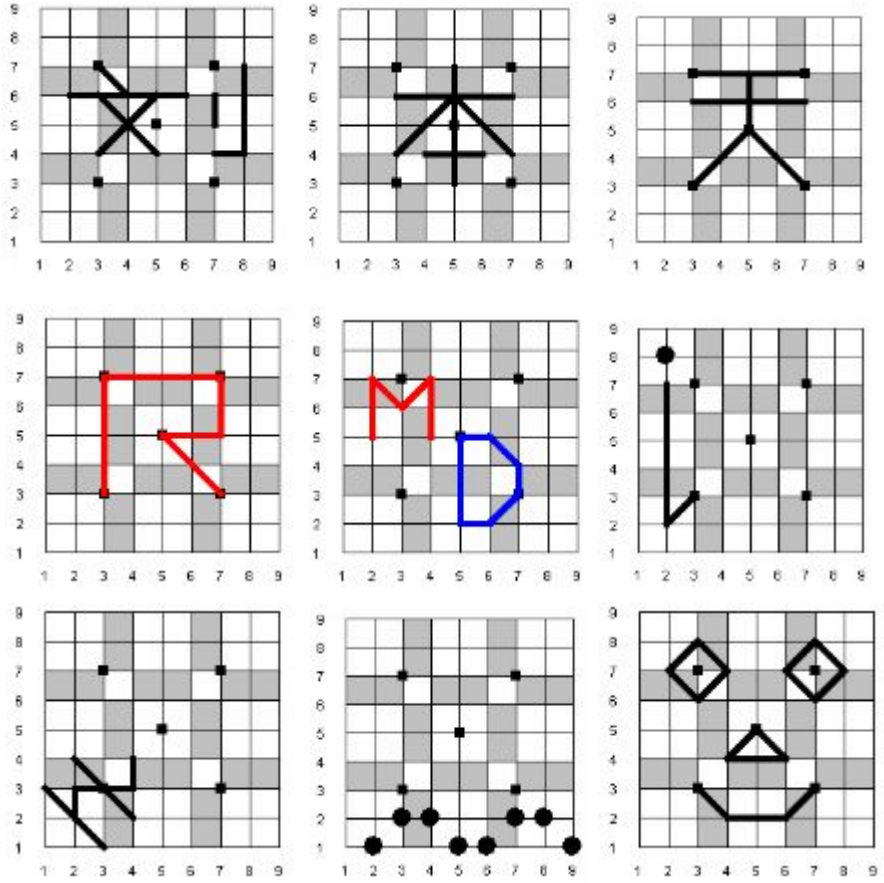
+ Mot de passe facile à retenir
+ BDAS mémorisation + efficace
- Les lignes et angles posent problème

Sécurité

+ Résistant aux Dictionary/Brute Force Attacks
- Shoulder Surfing non résolu
- Vulnérable aux Smudge Attacks et Spywares
- Souvent mêmes cases

Utilisabilité

+ Grille avec repères pour orienter l'utilisateur
+ Motifs faciles à retenir
- Certains motifs peuvent être difficile à retenir



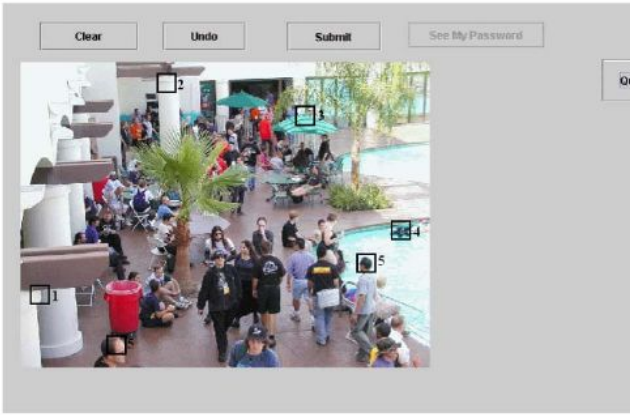
Passpoints

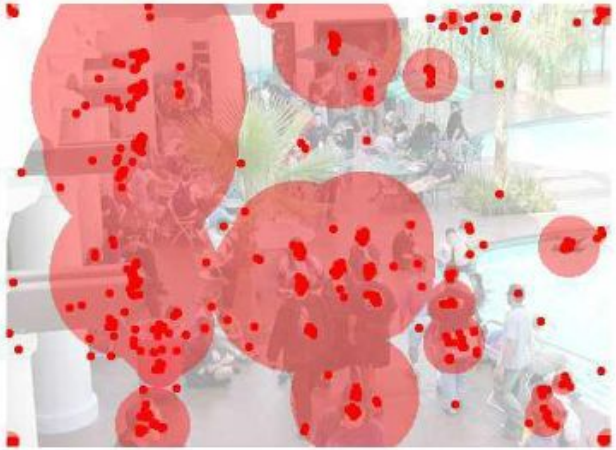
Sécurité

+ Résistant aux Brute force Attacks
- Vulnérable aux Smudge Attacks
- Vulnérable aux Dictionary Attacks (mêmes points)

Utilisabilité

+ Le taux de réussite 80%
+ Le temps de saisie rapide
+ La pratique améliore la précision
- Le choix de l'image peut influencer le taux de réussite
- L'utilisateur cache l'image avec son doigt
  -> sélection imprécise





Android Pattern Lock




Sécurité

+ Système de blocage généralement utilisé
+ Donc assez efficace contre Brute Force Attacks et Dictionary Attacks
- Très sensible aux Smudge Attacks et au Shoulder Surfing
- Habitude des utilisateurs



Utilisabilité

+ Authentification très rapide
+ Difficile de se tromper
- Certains segments sont difficiles a effectuer

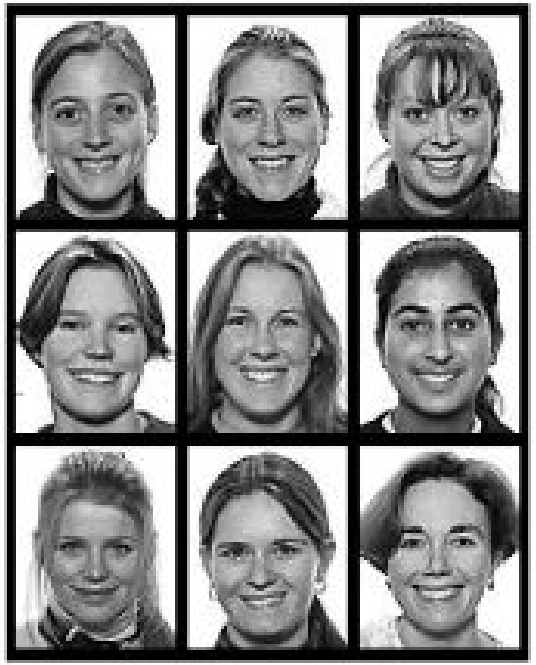
Passfaces

Sécurité

+ Dur à transmettre
- Sensible aux Brute Force Attacks (si aucun blocage)
- Vulnérable aux Guessing Attacks et Dictionary Attacks

Utilisabilité

+ Très bonne mémorisation (mieux que les textes)
+ Taux erreur trois fois moins élevé que les mots de passes classiques
- Temps d'authentification plus élevé que les mots de passe textuel



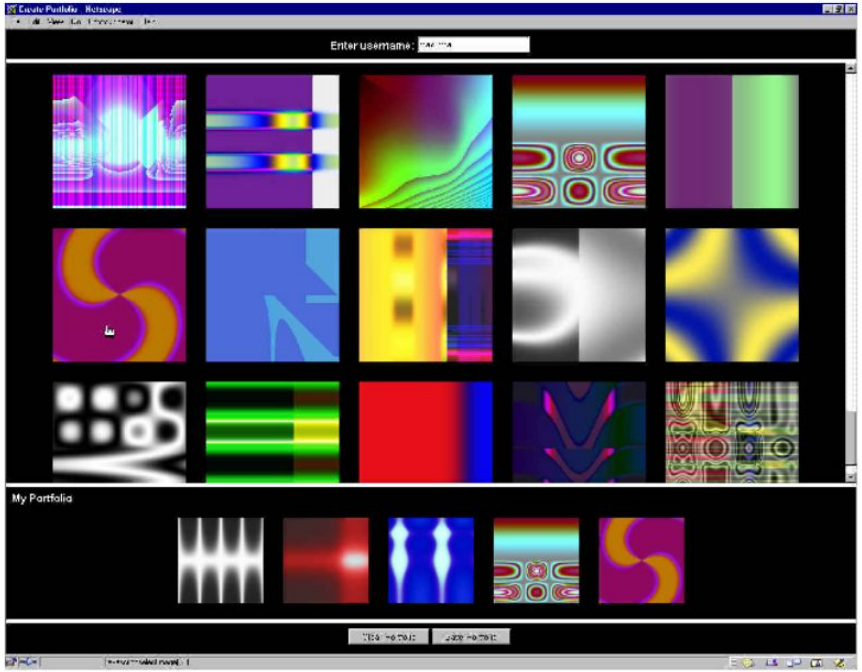
Déjà Vu

Sécurité

+ Résistant aux Brute Force attacks, Dictionary attacks
+ Difficile à partager
- Vulnérable si portfolio connu

Utilisabilité

+/- Temps d'authentification
+ Faible % d'erreur
- Création du portfolio assez longue



Convex Hull Click

Sécurité

+ Très résistant au Shoulder Surfing
+ Résistant aux Smudge attacks
- Faiblesse aux Guessing Attack

Utilisabilité

+ Facile à retenir
+ Taux d'erreur très faible
- Peut être très long de s'authentifier
- Zone difficilement cliquable peut survenir
- L'utilisateur cache l'image avec son doigt
  -> sélection imprécise

ColorLogin Graphical

Sécurité

- +/- Résistant aux attaques par Shoulder Surfing mais pas invulnérable si l'attaquant est rapide
- \+ Les couleurs permettent d'embrouiller l'attaquant
- \+ Le blocage de ligne empêche l'attaquant de connaître les icônes du mot de passe

Utilisabilité

- \+ Les couleurs aident l'utilisateur
- \- Long à déverrouiller si beaucoup d'étapes

Tableaux synthétiques

Nom du système	Catégorie	Brute Force Attack	Dictionary Attack	Shoulder Surfing	Smudge Attack	Eye tracking	Spyware, Keylogger	Espace de mot de passe	Indice de sécurité
Alphanumérique	rappel pur	3	3	2	5	5	0	3	3,00
Convex Hull Click	reconnaissance	3	5	5	5	0	5	3	3,71
Draw-A-Secret	rappel pur	3	3	2	2	0	3	3	2,29
Background DAS	rappel Indicé	3	3	2	2	0	3	3	2,29
Rotational DAS	rappel pur	5	3	3	3	3	3	3	3,29
Android Pattern Lock	rappel pur	0	3	0	2	3	0	1	1,29
Passfaces	reconnaissance	0	2	2	5	3	3	1	2,29
Déjà Vu	reconnaissance	0	2	2	5	3	3	1	2,29
Passpoint	rappel indicé	3	3	0	0	3	2	3	2,00
Pass-Go	rappel pur	3	3	2	2	3	2	3	2,57
ColorLogin Graphical	reconnaissance	0	2	3	5	5	3	2	2,86

Nom du système	Catégorie	Efficience (efficiency)			Efficacité (effectiveness)	Satisfaction	Indice d'utilisabilité
		Apprentissage	Mémorisation	Temps d'authentification			
Alphanumérique	rappel pur	2	2	3		3	2,5
Convex Hull Click	reconnaissance	2	3	0		3	2
Draw-A-Secret	rappel pur	5	3	5		5	4,5
Background DAS	rappel indicé	5	3	5		5	4,5
Rotational DAS	rappel pur	3	3	3		3	3
Android Pattern Lock	rappel pur	5	3	5		5	4,5
Passfaces	reconnaissance	5	3	3		3	3,5
Déjà Vu	reconnaissance	2	3	3		3	2,75
Passpoint	rappel indicé	3	3	3		3	3
Pass-Go	rappel pur	3	2	3		3	2,75
ColorLogin Graphical	reconnaissance	2	3	3		3	2,75

Conclusion

Projet.
Sécurité et utilisabilité :
le cas des mots de passe graphiques

Plan détaillé

1. Le projet
   a. Rappel du sujet
   b. Évolution du sujet
   c. Liste des exigences

2. Notre réalisation
   a. Essai de notre application
   b. L'accueil
   c. Les méthodes implémentées

3. Démarche, organisation
   a. Cycle de développement
   b. Planning et charges, prévu et réel
   c. Les rôles dans l'équipe
   d. Communication et réunions
   e. Livrables et recette
   f. Les outils utilisés

4. Conception
   a. Architecture
   b. La base de données
   c. Modularité et réutilisabilité
   d. Problèmes rencontrés

5. Conclusion et perspectives
   a. Conclusion et perspectives
   b. Remerciements

Sujet du projet

- En complément du sujet de TER
- Application Android ou JS, assez libre pour le choix final de l'application
- Seule exigence : mettre en avant les avantages et les inconvénients sur des méthodes d'authentification graphiques sur les aspects sécurité et utilisabilité

Définition précise du sujet

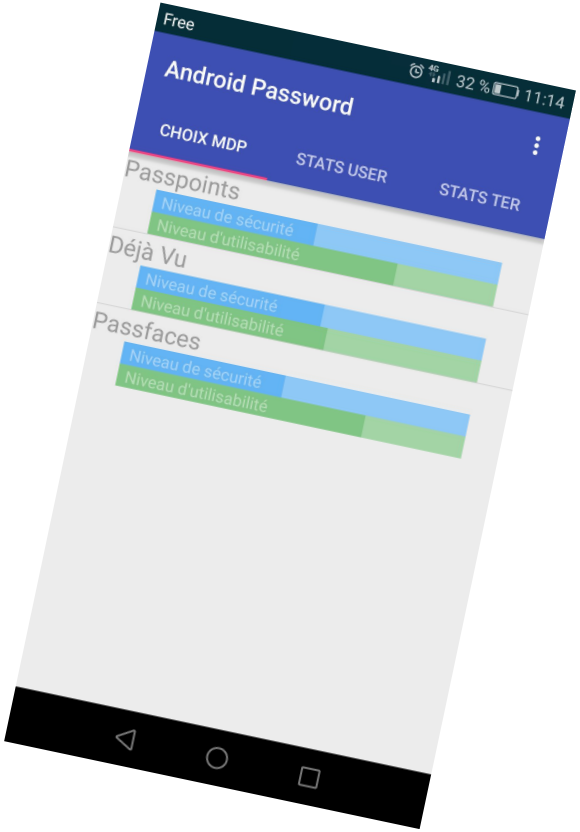
- Après que le TER ait avancé
- Au début … “implémenter un mot de passe innovant”
- Puis “développer une application d’authentification graphique existante avant de développer nos propres applications”
- Idée finale : **application permettant de découvrir, tester et comparer différents systèmes d’authentifications**

Les exigences

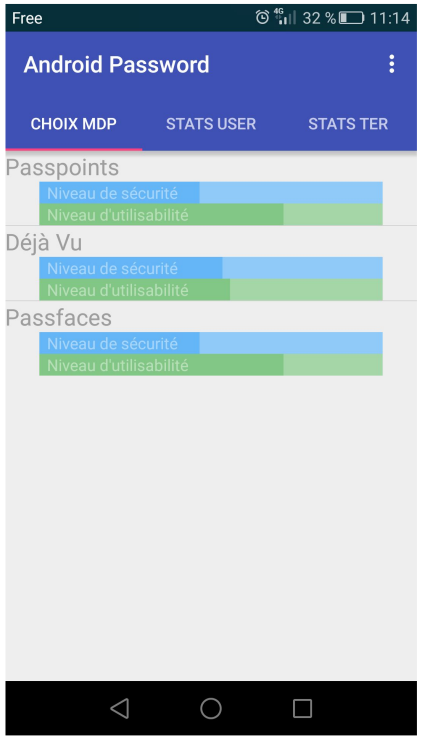
Numéro	Liste des exigences des parties prenantes
EF1	Le produit doit implémenter des méthodes d'authentifications graphique
EF2	L'application doit donner accès à la description des méthodes d'authentification (fonctionnement, menaces couvertes, indices de sécurité et d'utilisabilité...)
EF3	L'application doit permettre de tester ces mêmes méthodes d'authentification
EF4	L'application doit afficher le niveau de sécurité du mot de passe lors de sa création
EF5	Une méthode d'authentification peut être paramétrée
EF6	Le produit affiche un log de retour sur le test venant d'être effectué
EF7	L'application doit permettre de changer de méthode d'authentification et de mot de passe
EF8	L'application doit permettre de comparer les résultats de l'utilisation sur les différents systèmes d'authentifications
ENF1	Le produit doit être une application JAVA Android
ENF2	Le produit doit reprendre des résultats du TER fait conjointement
ENF3	Le produit doit permettre d'intégrer une nouvelle méthode d'authentification (réutilisabilité/modularité)

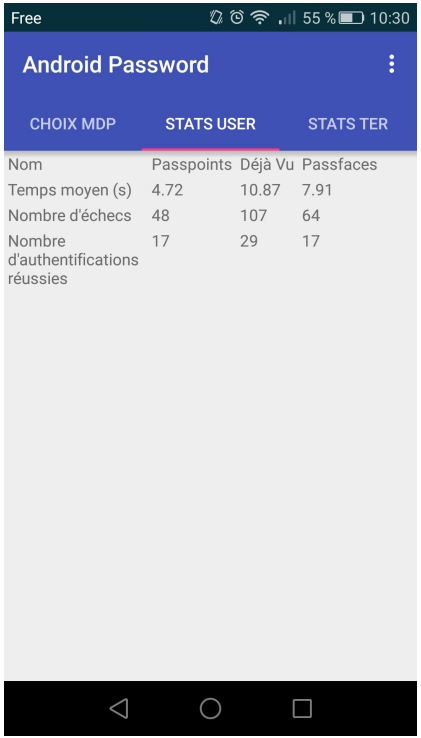
Réalisations

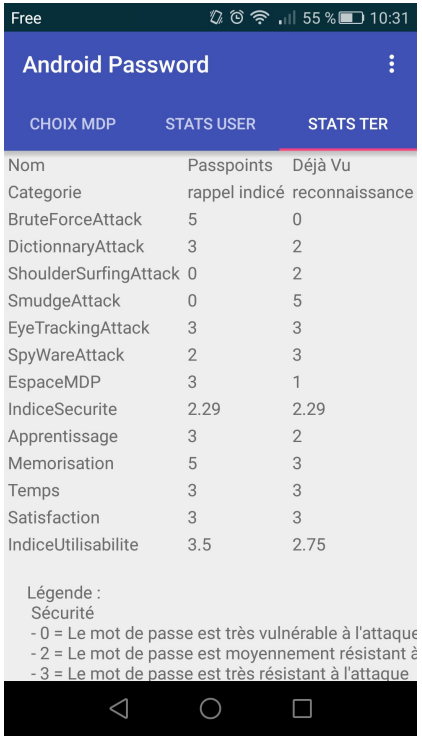
Réalisations



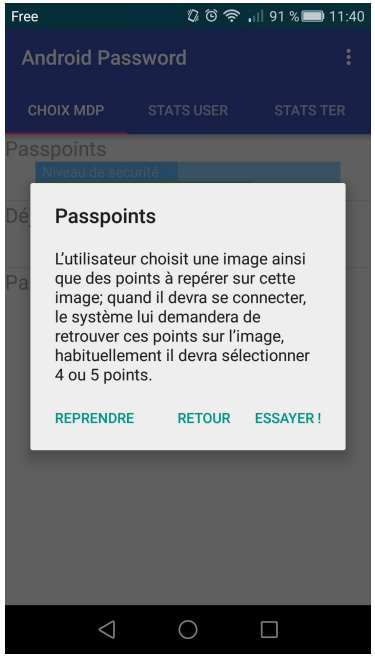
Accueil


Free
32 %
11:14
Android Password
CHOIX MDP
STATS USER
STATS TER
Passpoints
Niveau de sécurité
Niveau d'utilisabilité
Déjà Vu
Niveau de sécurité
Niveau d'utilisabilité
Passfaces
Niveau de sécurité
Niveau d'utilisabilité

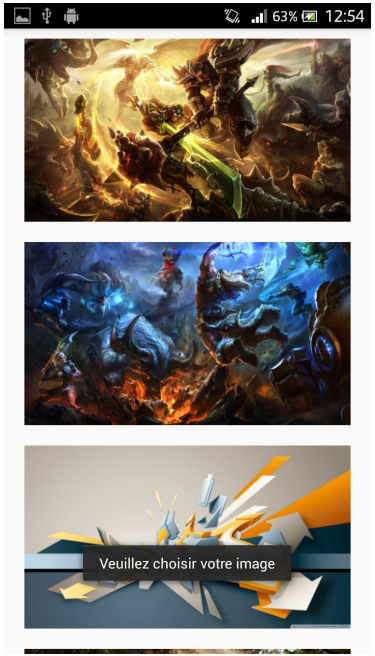

Free
55 %
10:30
Android Password
CHOIX MDP
STATS USER
STATS TER
Nom Passpoints Déjà Vu Passfaces
Temps moyen (s) 4.72 10.87 7.91
Nombre d'échecs 48 107 64
Nombre d'authentifications réussies 17 29 17


Free
55 %
10:31
Android Password
CHOIX MDP
STATS USER
STATS TER
Nom Passpoints Déjà Vu
Categorie rappel indicé reconnaissance
BruteForceAttack 5 0
DictionnaryAttack 3 2
ShoulderSurfingAttack 0 2
SmudgeAttack 0 5
EyeTrackingAttack 3 3
SpyWareAttack 2 3
EspaceMDP 3 1
IndiceSecurite 2.29 2.29
Apprentissage 3 2
Memorisation 5 3
Temps 3 3
Satisfaction 3 3
IndiceUtilisabilite 3.5 2.75
Légende :
Sécurité
- 0 = Le mot de passe est très vulnérable à l'attaque
- 2 = Le mot de passe est moyennement résistant à
- 3 = Le mot de passe est très résistant à l'attaque

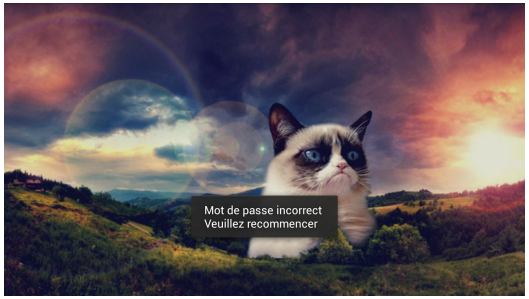
Sélection



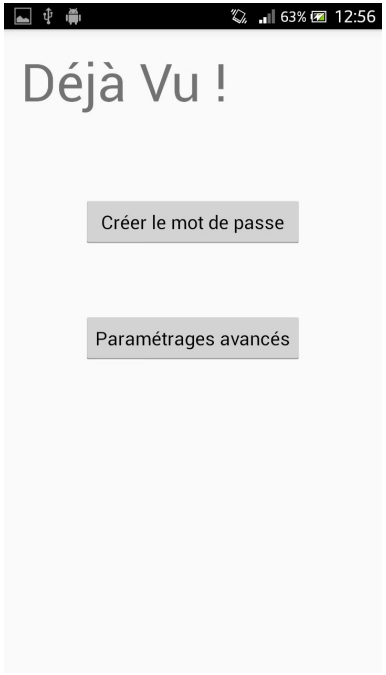
Création

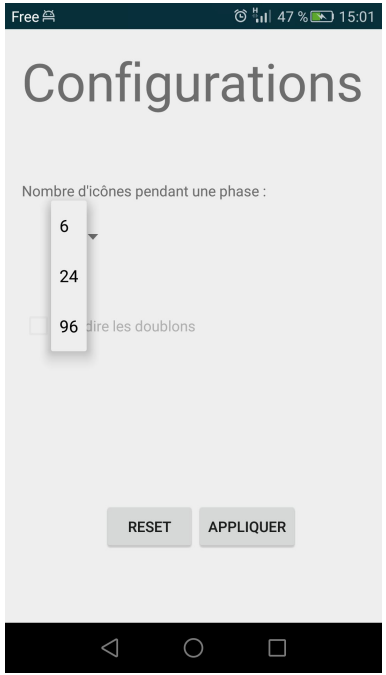


Authentification

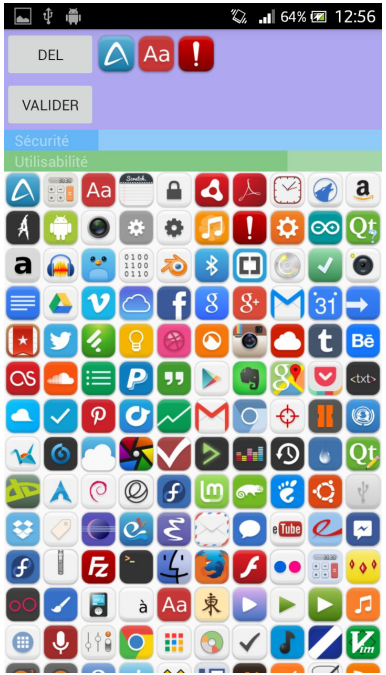


Configurations

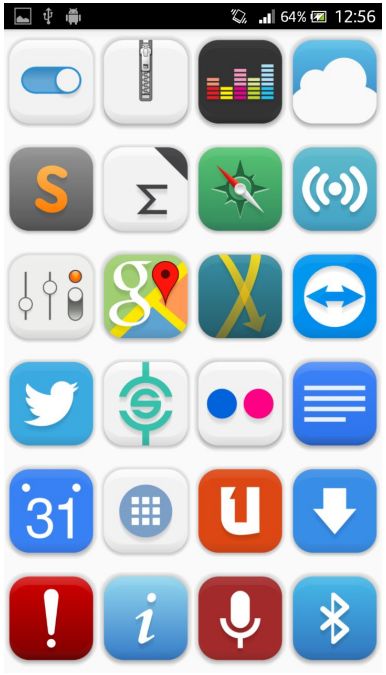




Création

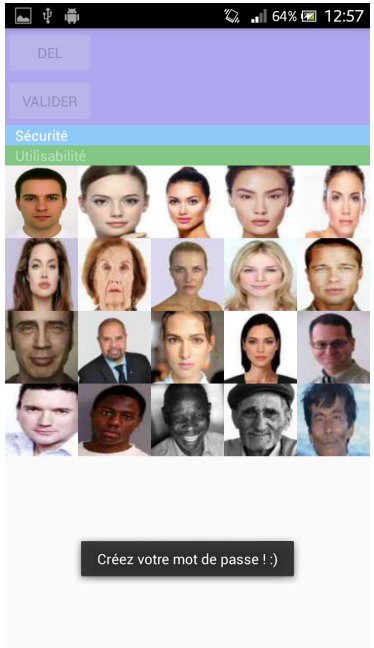


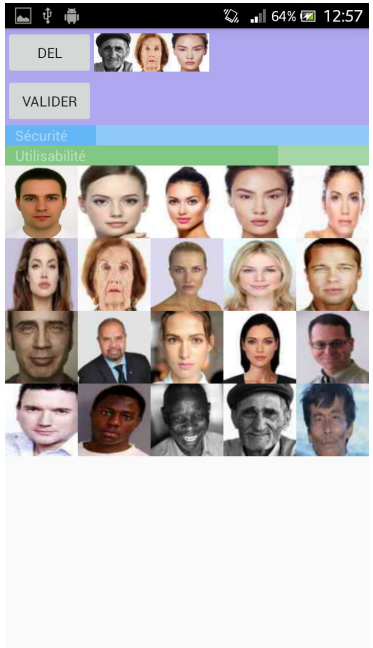
Authentification



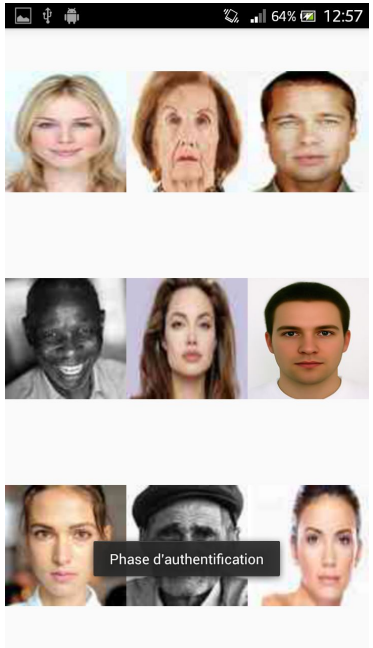
Passfaces

Création



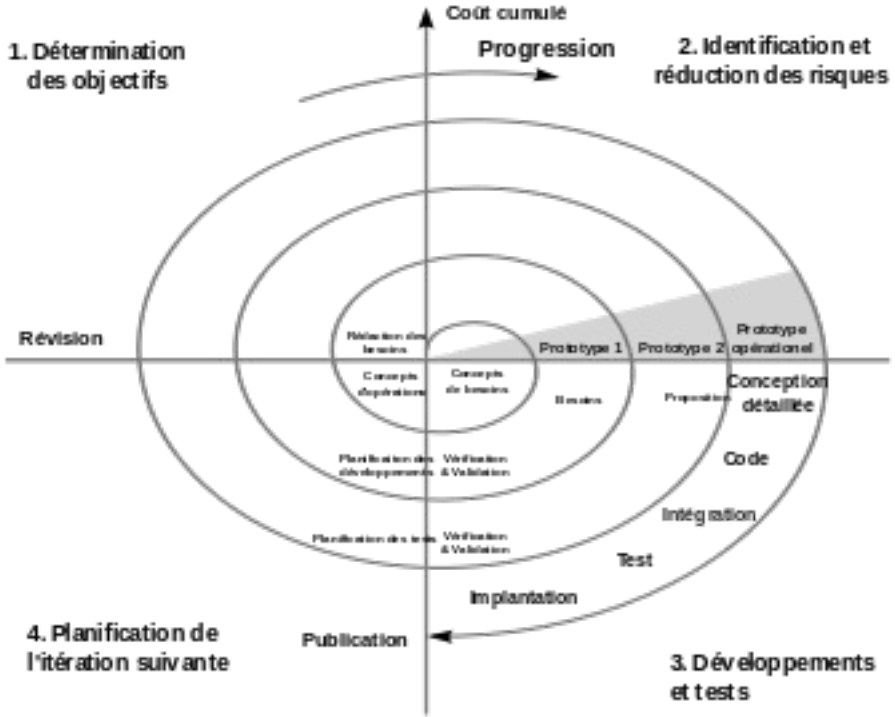


Authentification



Démarche, organisation

Cycle de développement

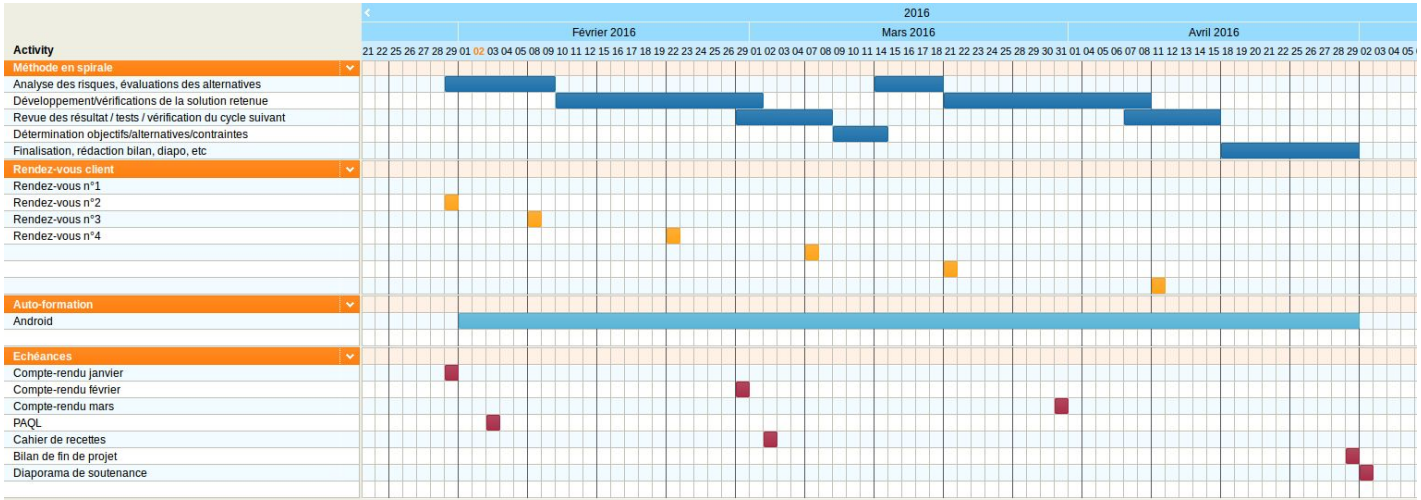


4 itérations :

- Itération 1 : Développement de Déjà Vu, Passpoints, Passfaces
- Itération 2 : Développement de la base de données et de l'accueil
- Itération 3 : Mise à jour graphique de l'accueil, des données TER et statistiques générés dynamiquement
- Itération 4 : Légères corrections après la dernière réunion

Planning et charges

Planning prévisionnel



Charge prévue
pour le groupe : ~ 150h

Réel

- Plus d'itérations, plus courtes
- Interruption pour les partiels

Charge réelle pour le groupe : ~ 220h
(pour le développement uniquement)

Les rôles dans l’équipe

Chef de projet : Matteo Mougeot

- a géré la communication entre son équipe et le client
- a organisé des réunions régulières avec son équipe, et avec le client
- a validé les documents du responsable documentation

Responsable technique : Benjamin Lacheray

- a proposé des plans d’implémentation du projet
- a assuré la coordination et le bon déroulement de la conception

Responsable qualité : Pierre Jeanmougin

- s’est assuré que les exigences soient respectées tout au long du projet
- a effectué des tests pour vérifier toutes les fonctions du produit

Responsable documentation : Lilian Le Quéré

- a créé et vérifié l’ensemble des documents, en veillant à leur qualité et à leur complétude
- s’est assuré qu’ils soient rendus dans les délais

Travail collaboratif

MBPL

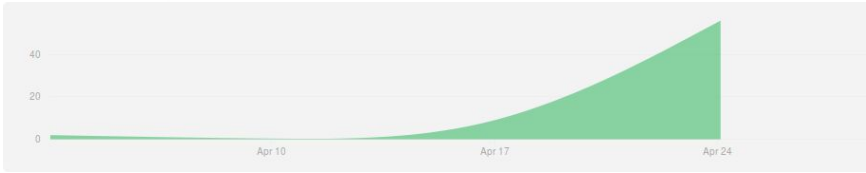
https://github.com/MBPL

Repositories | People 4 | Teams 1 | Settings

Application

MBPL's application to show some graphical passwords.

Updated a day ago



73 commits

bdd

Updated 4 days ago

8 commits

Deja-Vu

Méthode d'authentification "Déjà Vu"

Updated 20 days ago

7 commits

Communication et réunions avec le client

Communication

En interne : mail, skype, rdv réguliers à l'université
En externe : mail

Réunions

8 réunions avec M. Palanque Philippe du début jusqu'à la fin du projet, soit de mi **janvier** jusqu'à la recette le **28 avril**

Environ une réunion toutes les 2 semaines

Interruption du projet pendant environ 3 semaines avant et pendant les partiels

Recette le 28/04/2016

Livrables

Au corps enseignant et au client (respectivement sur Moodle et sur Google Drive) :

- ❏ Comptes-rendus mensuels x3 (Janvier, Février, Mars)
- ❏ Plan d'Assurance Qualité Logicielle
- ❏ Cahier de Recette
- ❏ Bilan du projet

Au client sur Google Drive :

- ❏ Application fonctionnelle (installeur .apk)
- ❏ Guide d’ajout d’une nouvelle méthode
- ❏ Code source
- ❏ Comptes-rendus des réunions
- ❏ Compte-rendu de recette et améliorations apportées

Éléments de contrôle	Appréciation du client
T1 : Le produit implémente au moins deux méthodes d'authentifications graphiques	Ok 28/04/2016
T2 : L'application donne accès à la description de la méthode d'authentification "Déjà Vu"	Ok
T3 : L'application permet de tester la méthode d'authentification "Déjà Vu"	Ok
T4 : L'application affiche le niveau de sécurité du mot de passe lors de sa création	Ok mais pas compréhensible
T5 : L'application permet de changer le nombre d'image à l'authentification de "Déjà Vu"	Ok
T6 : Le produit affiche un log de retour sur le test venant d'être effectué	Ok (pas sur le test, dans onglet log)
T7 : L'application permet de changer de méthode d'authentification	Ok
T8 : L'application permet de comparer les résultats de l'utilisation sur les différents systèmes d'authentifications	Ok - pas très clair
T9 : Le produit est une application JAVA Android	Ok
T10 : Le produit reprend des résultats du TER fait conjointement	Ok
T11 : Le produit permet d'intégrer une nouvelle méthode d'authentification	Ok (pas testé)

Outils et technologies utilisés

https://github.com/MBPL

git

GitHub

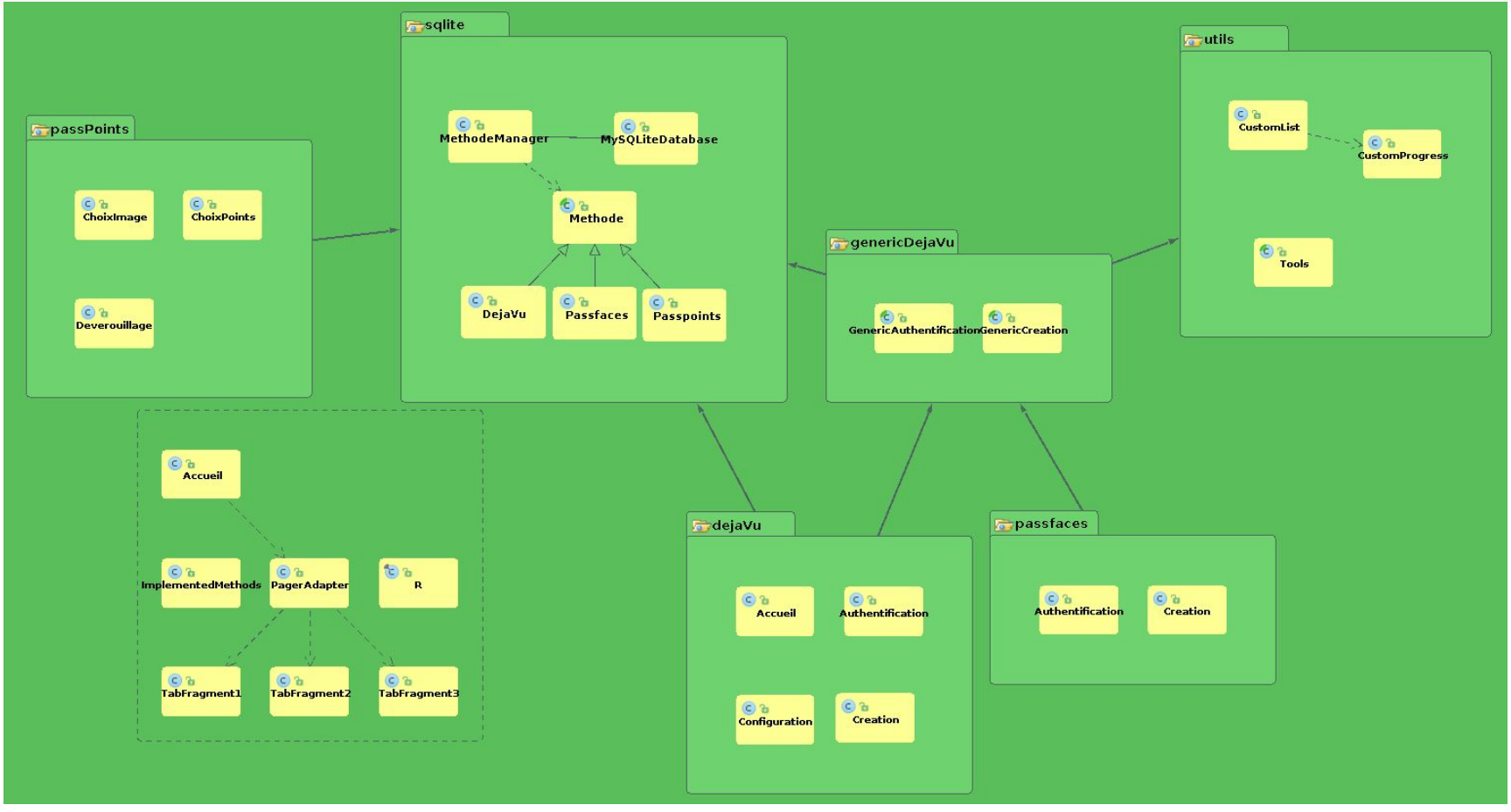
Google Drive

Android Studio

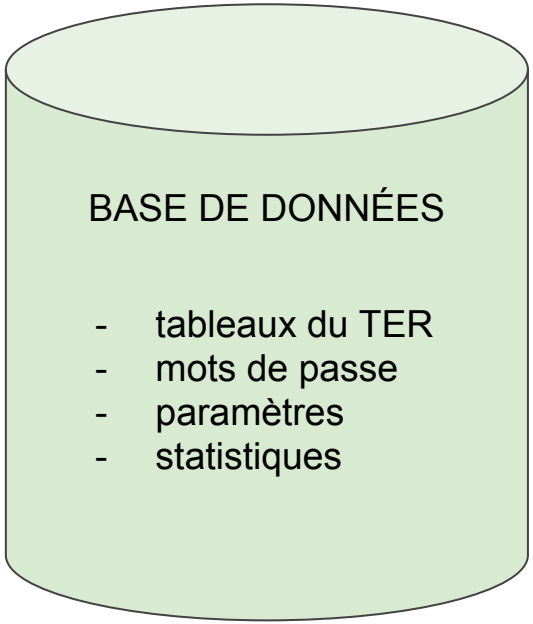
SQLite

Détails sur la conception

Vue packages et classes



Détails sur la base de données



Réutilisabilité, modularité

Notre conception permet d'**intégrer facilement** des **nouvelles méthodes** d'authentifications.

Les classes du package genericDejaVu permettent d'**implémenter facilement** des méthodes de **type "Déjà Vu"**.

D'autres composants du système sont réutilisables.

Limites : Patterns ? Arch-Slinky ?

Problèmes rencontrés

- Anecdote : l’indicateur de chargement...
- Installation d’Android Studio (sur windows)
- Android était un environnement inconnu

Conclusion et perspectives

Ce que nous avons appris

- Sensibilisation aux notions de sécurité et d'utilisabilité
- Découverte puis bonne prise en main d'Android
- Mise en application de nos connaissances
- Expérience scolaire qui se rapproche le plus d'une vraie gestion de projet

Perspectives

L'application pourrait être amélioré et enrichie de nouvelles méthodes.

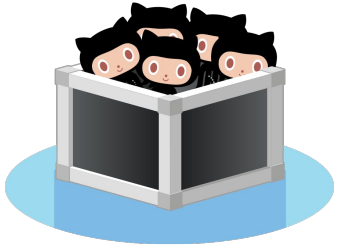
Idées d'autres usages de l'application :
- pourrait être utile pour des tests utilisateur sur de nouvelles méthodes
- pourrait permettre d'intégrer une méthode directement au système Android de l'utilisateur

Remerciements

Merci à M. Palanque Philippe pour sa disponibilité, son aide et sa constante bonne humeur.

Merci à Mme Martinie Célia pour ses indications dans le développement Android.

Et merci à tout le corps enseignant !



Fin