



Ingénieurs 2000 – IR3
Projet de génie logiciel

Shieldroid

Sécurité Embarquée sur PDA



Cahier des charges graphique

Version	Type	Date
1.0	Initiale	17/11/2009
2.0	Correction des accès IG supplémentaires	23/11/2009

Clément Lecigne / Jordane Marcel / Jean-Christophe Rios / Willy Rouvre / Frédéric Tran

Sommaire

1	Introduction.....	3
2	Glossaire	4
3	Gestion des langues	9
4	Progress Bar pour les opérations longues.....	9
5	Navigation dans l'application	10
6	Icône d'accès aux paramètres Shieldroid.....	11
7	Menu Shieldroid	12
8	Paramétrage des menus	13
8.1	Accès aux paramètres des menus	13
8.2	Le paramétrage des menus	15
9	Menu Protection des données	16
9.1	Sous-menu Authentification.....	17
9.1.1	Demande d'authentification pour l'accès à un fichier.....	18
9.1.2	Notification d'erreur lors d'une authentification erronée.....	18
10	Menu d'Accès initial	19
10.1	Paramétrer les questions/réponses.....	20
10.2	Demande de réponse à l'accès initial	21
10.3	Message d'erreur accès initial	22
11	Menu Anti-Spam SMS	23
12	Menu Pare-feu	24
12.1	Pare-feu passif.....	24
12.1.1	Ajout d'une règle.....	25
12.2	Pare-feu réactif	26
12.2.1	Mise à jour du pare-feu réactif	27
13	Menu Communication sécurisée	28
13.1	Ajout d'une communication sécurisée par tunnel	29
14	Menu Logs (Journaux)	30
15	Notification pour les journaux	31
16	Menu paramétrage	34
17	Icône d'accès à la communication sécurisée utilisateur	36
18	Menu Communication Sécurisé pour utilisateur	37
19	Conclusion	38
20	Annexes	39
20.1	Vue globale	40

	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

1 Introduction

Le cahier des charges graphique est un dossier ayant pour but de présenter l'interface graphique de l'application. Le client pourra de cette manière avoir un aperçu des différentes fonctionnalités de l'application et ainsi donner son avis sur ce que sera la livraison graphique.

Dans la situation actuelle, les différentes interfaces graphiques ne sont pas encore développées. Il s'agit de captures d'écran réalisées à l'aide de différents outils en java qui se base sur l'interface graphique de base du système Android. Il est donc important de noter qu'il s'agit d'une interface globale de ce que sera l'application. Ces captures ne définissent donc pas contractuellement l'interface graphique finale.

L'application ShieldDroid est un logiciel qui doit permettre de sécuriser les différents PDA fonctionnant sur le système Android.

Cette application se compose en plusieurs parties :

- Un accès générale à l'application avec :
 - un tableau de bord avec les statistiques de chaque module
 - un bouton pour accéder au paramétrage "administrateur" de l'application

- Un écran de paramétrage de l'application avec :
 - un bouton pour paramétrer chaque module avec la possibilité de l'activer/désactiver.
 - nécessité de s'authentifier pour y accéder.

L'objet de ce document est alors de donner un aperçu visuel de l'application et ainsi conserver une cohérence graphique dans les interfaces des différents composants du logiciel.

	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

2 Glossaire

Android:

Système d'exploitation libre pour et terminaux mobiles conçu par Android, une start-up rachetée par Google. Il a été annoncé le 15 novembre 2007. Afin de promouvoir ce système d'exploitation ouvert, Google a su fédérer autour de lui une trentaine de partenaires réunis au sein de l'Open Handset Alliance. Basé sur un noyau Linux, Android a été conçu pour intégrer au mieux des applications existantes de Google comme le service de courrier Gmail, ou celui de cartographie, Google Maps, ou encore Google Calendar, Google Talk, YouTube. Un accent particulier est mis sur la géolocalisation.

Anti-spam:

L'anti-spam désigne un ensemble de systèmes et moyens techniques de lutte contre le SPAM (publicité non sollicités envoyées par email, SMS, MMS).

API (Application Programming Interface)

Interface de développement fournie par une bibliothèque logicielle. Elle permet de définir la communication entre deux composants électroniques.

Authentification

L'authentification est un mécanisme qui permet de vérifier que l'utilisateur qui tente d'accéder au système est une personne autorisée. Le mécanisme repose sur un couple identifiant et mot de passe qui permettent de valider l'identité d'un utilisateur.

Bluetooth

Protocole de connexion par ondes radio entre appareils portables, ordinateurs, téléphones.

Checkbox

En français, une case à cocher, est un composant des interfaces graphiques permettant à l'utilisateur d'indiquer des choix.

	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

CVE (Common Vulnerabilities and Exposures)

Identifiant dans un dictionnaire des informations publiques relatives aux vulnérabilités de sécurité. Le dictionnaire est maintenu par l'organisme MITRE, soutenu par le Département de la Sécurité intérieure des États-Unis. Chaque vulnérabilité connue possède son propre CVE.

Framework

Ensemble de bibliothèques logicielles fournissant des fonctionnalités au programmeur au travers d'interfaces spécialement conçues.

Firewall

Pare-feu en français, métaphore utilisée pour désigner un logiciel et/ou matériel, qui a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant au moyen de règles quel trafic est considéré comme légitime en entrée ou sortie du réseau.

GSM (*Global System for Mobile Communications*)

Norme de communication radio répandue en Europe définissant un réseau cellulaire utilisé par les téléphones portables.

IHM (*Interface Homme Machine*)

Ensemble d'éléments constitutifs du système qui permettent l'interaction de l'utilisateur avec le système.

IP (Internet Protocol)

Internet Protocol. Protocole de transmission de données par le réseau. Les données sont véhiculées sous forme de paquets acheminés par des intermédiaires (routeurs).

IPSec (*Internet Protocol SECURITY*)

Ensemble de protocoles définis par l'IETF afin de chiffrer des paquets au niveau de la couche IP. Fondé sur un système à clef publique, il fonctionne selon deux modes possibles : « Transport » et « Tunnel ». Dans le premier cas, seule la charge utile des paquets est chiffrée, dans l'autre l'en-tête est lui aussi protégé.

	Projet de Génie Logiciel « Shieldroid »	TD2K
--	--	------

Java

Langage de programmation orienté objet multi plateforme.

LAND attack

Génère un flot de datagrammes UDP, de tailles variables, avec des adresses IP aléatoires. Ceci est en mesure de dérouter la cible et l'amener à une déconnexion du réseau suite à un ralentissement important de son trafic.

Linux

L'une des plus connues des versions de noyau de type Unix distribué sous une licence libre. Il est développé depuis 1991, tout d'abord par un étudiant finlandais nommé Linus Torvalds isolé, qui jugeait les tarifs des versions commerciales d'Unix rédhitoires. Il a su, via l'Internet, convaincre une ample communauté de l'aider. Le terme Linux désigne souvent un système complet (noyau Linux et les outils du système d'exploitation), appelé distribution.

Logiciel libre

Les logiciels libres sont des programmes ou bibliothèques associés à une licence (une sorte de contrat) garantissant à l'utilisateur du logiciel un certain nombre de libertés. Les logiciels associés à ce type de licence répondent à plusieurs libertés fondamentales. Ces libertés sont : la liberté d'exécution, le logiciel peut-être utilisé quel qu'en soit le but ; la liberté de modification, ce qui sous-entend que le code source du logiciel est fourni ; la liberté de redistribution, modifié ou non, le logiciel peut-être redistribué à quiconque, gratuitement ou non.

NetFilter

Framework implémentant un pare-feu au sein du noyau Linux à partir de la version 2.4 de ce dernier. Il prévoit des accroches dans le noyau pour l'interception et la manipulation des paquets réseau.

Noyau

Programme responsable de toutes les tâches de base du système d'exploitation, par exemple assurer l'accès à des ressources externes, l'ordonnancement des processus ou encore la gestion de la mémoire.

	Projet de Génie Logiciel « Shieldroid »	TD2K
--	--	------

OS fingerprinting

Littéralement "prise d'empreintes". Type d'"attaque" à distance qui vise à déterminer le système d'exploitation d'un hôte, en analysant par exemple ses réponses à des requêtes spécialement malformées.

PDA (Personal Digital Assistant)

Littéralement "assistant numérique personnel". C'est un appareil numérique portable et programmable.

PIN (Personal Identification Number)

Identifiant de quatre chiffres qui authentifie un utilisateur une carte SIM téléphonique. La saisie erronée de ce code peut conduire au blocage de la carte SIM.

POC (Proof Of Concept)

Littéralement "preuve du concept". C'est une étape dans le processus de développement d'une application. Elle permet au client d'avoir un aperçu du rendu final, sous forme de "maquette" proposant un nombre limité de fonctionnalités. Ceci afin de dégager la ligne conductrice du projet, et de pouvoir réellement démarrer la production sur des bases validées.

Progress Bar

Une barre de progression (ou barre de chargement) est un composant de base des interfaces graphiques qui permettent d'indiquer à l'utilisateur l'état d'avancement d'un travail qu'est en train d'effectuer l'ordinateur. Au début la barre est complètement vide, puis elle se remplit au fur et à mesure de l'avancement de la tâche pour finir complètement remplie lorsque le travail est terminé.

SDK (Software Development Kit)

Kit pour développer simplement des logiciels.

Système d'Exploitation

Operating System (OS) en anglais, c'est l'ensemble des logiciels de base, parfois très avancés, permettant l'usage optimal d'un ordinateur.

	Projet de Génie Logiciel « Shieldroid »	TD2K
--	--	------

Tableau de bord

Partie de l'interface graphique permettant au gestionnaire de visualiser l'avancement des étapes de la planification via des indicateurs.

TCP (Transmission Control Protocol)

Littéralement, « protocole de contrôle de transmissions » abrégé TCP, est un protocole de transport fiable, en mode connecté, documenté dans la RFC 793.

VPN (Virtual Private Network)

Dans les réseaux informatiques et les télécommunications, le réseau privé virtuel est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel ».

Vulnérabilité

Défaut d'un logiciel permettant une manœuvre théoriquement impossible ou interdite qui engendre un problème de sécurité.

WiFi

Technologie de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenu un moyen d'accès à haut débit à Internet.

3 Gestion des langues

Les interfaces graphiques sont présentées par défaut dans deux langues, l'anglais et le français. Cependant comme l'internationalisation est prévue de base dans le SDK d'Android, il sera assez aisé d'ajouter n'importe quelles autres langues. En effet, il suffira d'ajouter un fichier de configuration XML dans un dossier particulier.

Le logiciel Shieldroid s'adaptera en fonction de la langue configurée sur le téléphone pour son choix de langage par défaut. De plus, l'administrateur a la possibilité de forcer le langage dans l'interface de configuration du système Shieldroid.

4 Progress Bar pour les opérations longues

L'état d'avancement des opérations longues sera représenté par une barre de progression. Nous utiliserons la barre de progression sous forme de cercle qui est fournie dans les SDK d'Android.



5 Navigation dans l'application

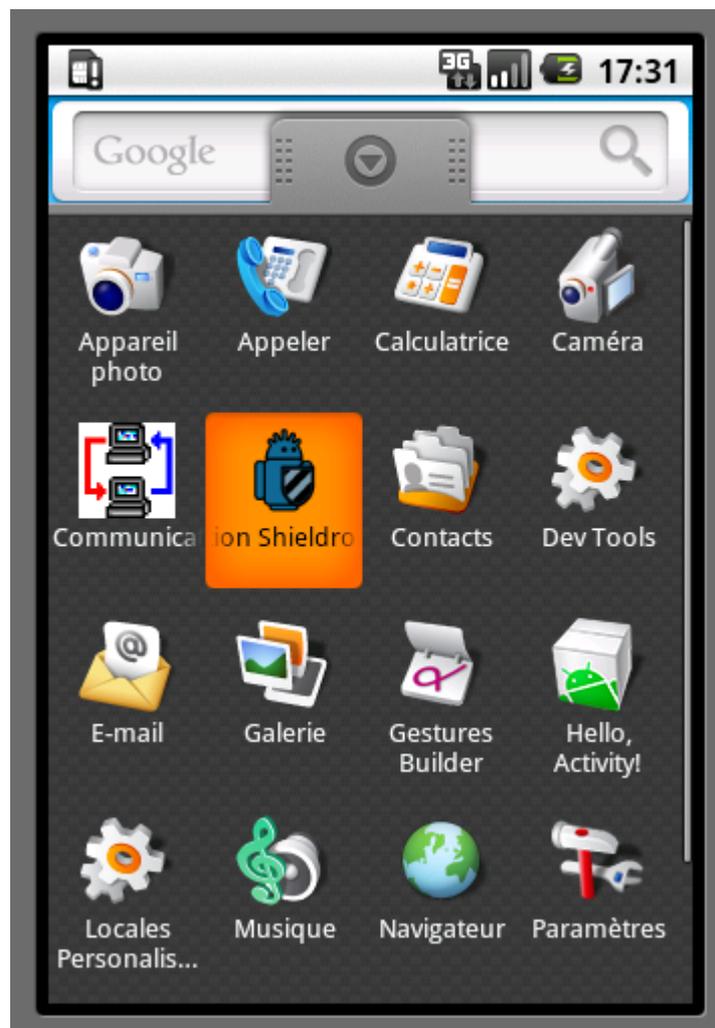
La navigation dans le logiciel Shieldroid sera conforme au standard de navigation sous Android. En effet, chaque téléphone prévoit un bouton retour pour revenir à l'écran précédent. Ce bouton sera pris en compte dans notre application.



	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

6 Icône d'accès aux paramètres Shieldroid

Notre application est accessible au même titre que les autres applications. Elle possède une icône particulière et un nom qui permet de l'identifier facilement. Un clic sur cette dernière ouvre l'application. Cette icône possède un texte défilant qui affiche « Configuration Shieldroid ».

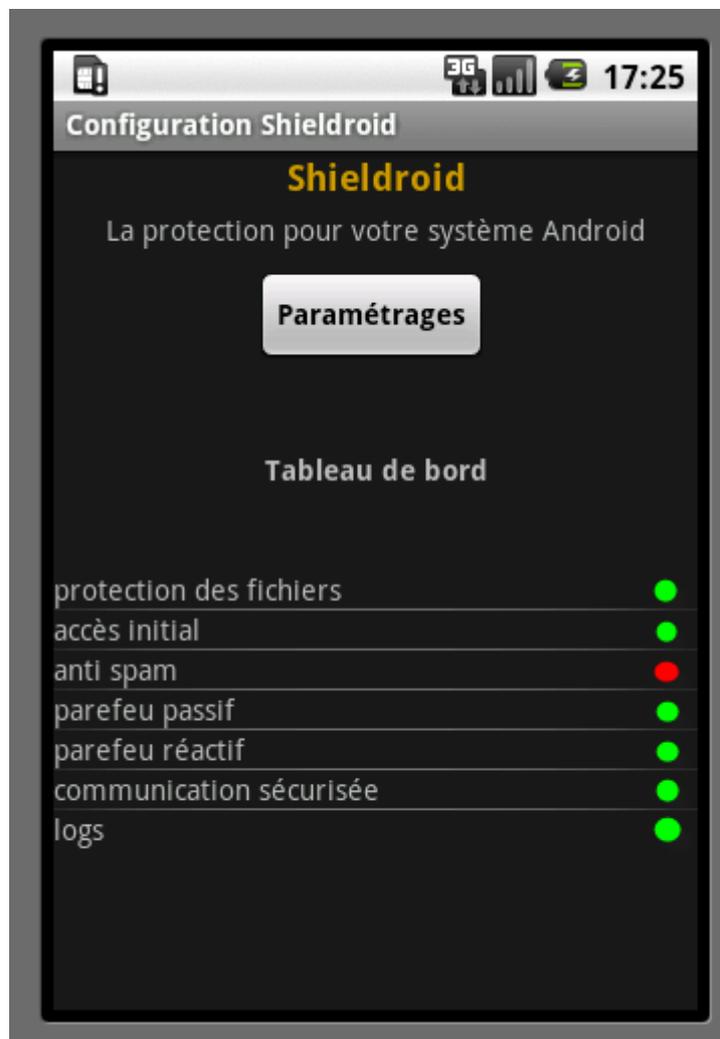


7 Menu Shieldroid

La première interface présentée lorsque l'on ouvre l'application possède:

- un tableau de bord qui présente les informations générales sur le système Shieldroid
- un lien (sous forme de bouton dans l'interface présentée) pour accéder au module de paramétrage des fonctionnalités.

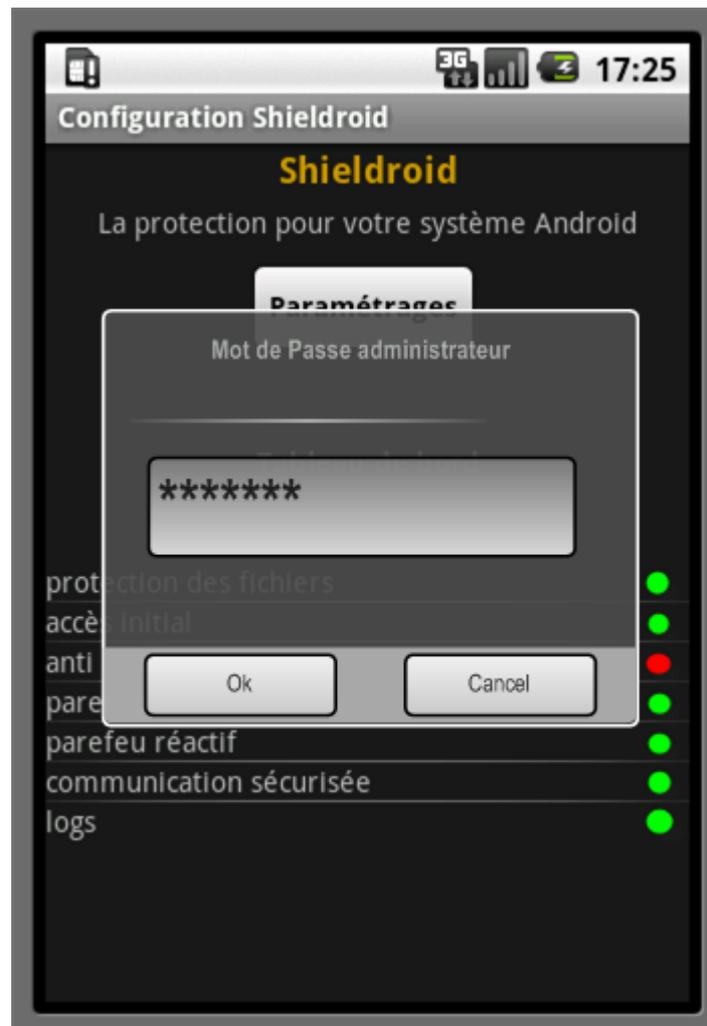
Le tableau de bord sur cet exemple d'interface affiche les modules qui sont actifs et inactifs.



8 Paramétrage des menus

8.1 Accès aux paramètres des menus

Lorsque l'on tente d'accéder aux paramètres des menus, le clavier s'active et un prompt demandant à l'utilisateur de renseigner le mot de passe de l'administrateur est ouvert.



	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

Si le mot de passe est incorrect, un message d'erreur est affiché et on retourne à l'écran principal de shieldroid.



8.2 Le paramétrage des menus

L'interface de paramétrage des menus de sécurité affiche séparément un lien sous forme de bouton pour accéder au paramétrage de chaque module. Depuis cette interface, tous les modules peuvent être activés ou désactivés en cliquant sur la checkbox correspondante. Si un module est désactivé alors le lien pour paramétrer ce module ne fonctionne pas.



On remarque sur cet exemple que le module Anti-Spam a été désactivé

	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

9 Menu Protection des données

Le module de protection des fichiers propose 3 sous menus pour accéder aux paramètres de l'authentification, de la confidentialité ou du contrôle d'intégrité sur les fichiers. L'interface propose aussi un lien "logs" pour accéder aux journaux associés à ce module.



Un lien direct vers les logs de ce module est disponible, en bas du menu.

9.1 Sous-menu Authentification

L'interface de paramétrage de l'authentification sur les fichiers liste les ressources sous protection par authentification et si cette dernière est active. Un flag précise pour chaque entrée si c'est un fichier (F) ou un répertoire (D). Un bouton permet de supprimer une entrée et un autre bouton permet d'ajouter une nouvelle entrée.



	Projet de Génie Logiciel « Shieldroid »	TD2K
--	--	------

9.1.1 Demande d'authentification pour l'accès à un fichier

Lorsque l'on tente d'accéder à une ressource sous une protection par authentification, un prompt demandant le mot de passe de l'administrateur est ouvert.



9.1.2 Notification d'erreur lors d'une authentification erronée

Si le mot de passe rentré n'est pas correct alors un message d'erreur de ce type est renvoyé à l'utilisateur et la ressource n'est pas ouverte.



 shieldroid	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

10 Menu d'Accès initial

Le paramétrage du menu d'accès initial propose un lien pour ajouter, supprimer ou lister des questions, de paramétrer le nombre de questions posées à chaque déclenchement du module et de paramétrer le nombre de tentatives autorisés par question avant le blocage du téléphone. Le nombre de questions demandées est paramétrable à l'aide d'une liste déroulante, allant de 1 à 5. Le nombre de tentatives autorisées avec le blocage du système est paramétrable à l'aide d'une liste déroulante, allant de 1 à 5.



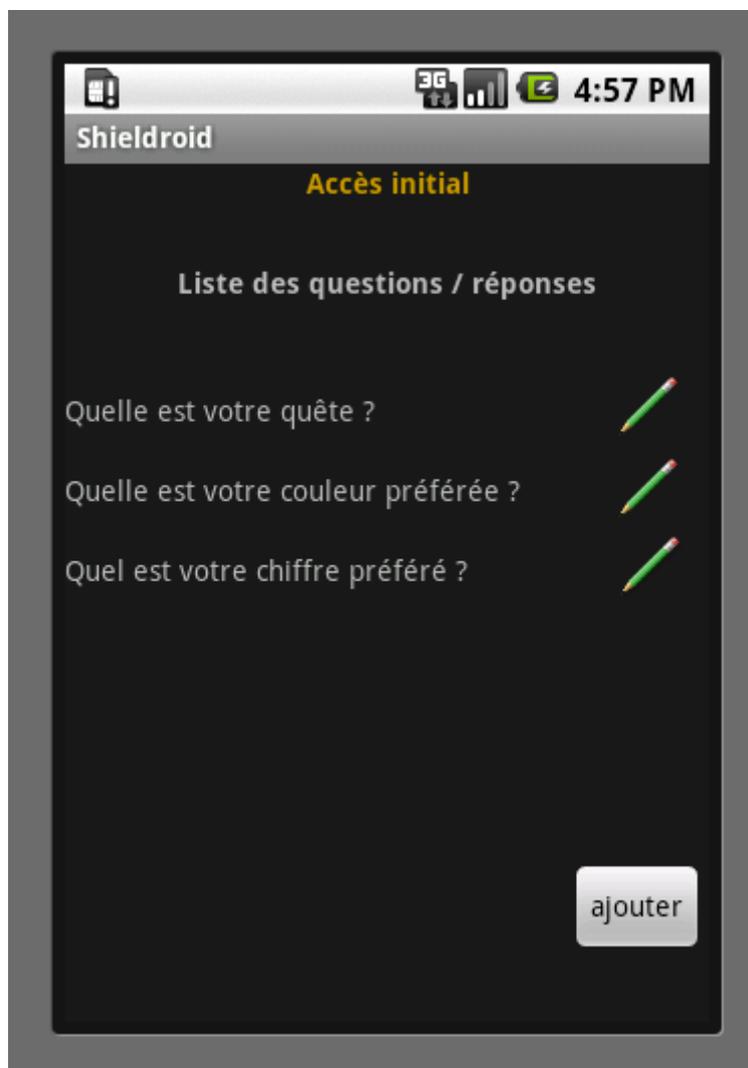
Un lien direct vers les logs de ce module est disponible, en bas du menu.

	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

10.1 Paramétrer les questions/réponses

Lorsque l'on accède à paramétrage des questions, nous avons le listing de toutes les questions configurées dans le module d'accès initial et la possibilité d'ajouter de nouvelles questions. Pour chacune des questions listées, un bouton en forme de crayon permet de :

- visualiser la réponse correspondante
- modifier la réponse correspondante
- supprimer le couple question / réponse



10.2 Demande de réponse à l'accès initial

Lors du déclenchement du module d'accès initial, le système retourne et se verrouille sur la page d'accueil d'Android et propose des questions à l'utilisateur auquel il doit répondre pour pouvoir retrouver un système fonctionnel. La question est présentée de la forme suivante :



	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

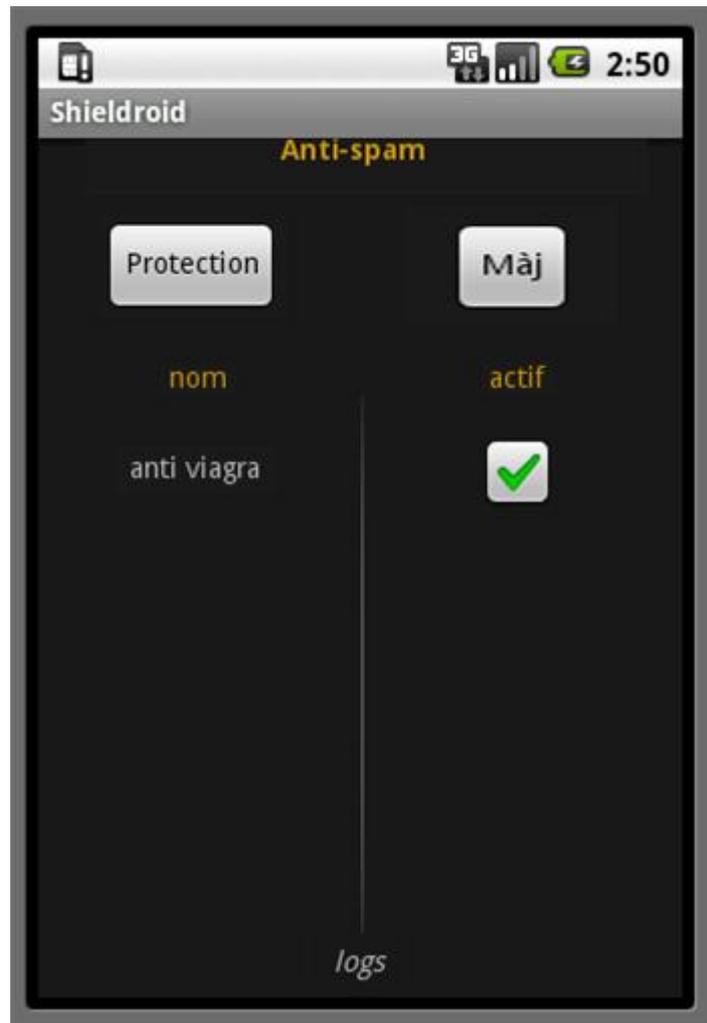
10.3 Message d'erreur accès initial

Si l'utilisateur échoue dans le module d'accès initial, le système Shieldroid lui répond avec une erreur de la manière suivante et le téléphone rentre en mode "blocage".



11 Menu Anti-Spam SMS

L'écran principal de configuration du menu anti-spam ne fait que lister la liste des protections contre le spam qui sont active dans le module. L'administrateur à la possibilité d'activer ou désactiver chaque protection. L'interface propose également un lien pour paramétrer les mises à jour des protections du module anti-spam dans lequel l'administrateur peut spécifier le serveur de mise à jour et la fréquence de mise à jour des protections.



Sur cette interface, nous avons la protection contre les messages SMS de publicité pour du viagra qui est activé.

Un lien direct vers les logs de ce module est disponible, en bas du menu.

12 Menu Pare-feu

12.1 Pare-feu passif

La configuration du menu pare-feu passif présente la liste des règles qui sont configurées dans le système Shieldroid. Il affiche les attributs (sur cette interface, tous les attributs ne sont pas affichés) de chaque règle avec la possibilité d'en supprimer, d'en modifier. Un bouton ajouter une nouvelle règle permet d'entrer dans une nouvelle interface pour ajouter des règles.



Un lien direct vers les logs de ce module est disponible, en bas du menu.

 shieldroid	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

12.1.1 Ajout d'une règle

L'interface d'ajout d'une nouvelle règle dans le pare-feu propose l'édition de chaque attribut (tous les attributs n'ont pas été présentés sur l'interface) d'une règle. Certains attributs comme le protocole sont présentés à l'utilisateur sous forme d'une liste déroulante.

Les champs d'adresse devront respecter la forme d'une adresse IP.



The screenshot shows a mobile application window titled "Shieldroid" with a status bar at the top showing the time as 2:26. The main content area is titled "Parefeu passif" and "Ajout d'une règle". It contains four input fields for rule configuration: "adresse source", "adresse destination", "port source", and "port destination". Each field is currently empty. At the bottom of the form is an "OK" button.

12.2 Pare-feu réactif

Comme le menu d'anti-spam, le module de configuration du pare-feu réactif liste les protections configurées sur le système avec la possibilité de les activer ou de les désactiver. L'interface propose un lien vers le paramétrage de la mise à jour automatique des protections et un lien pour ajouter manuellement de nouvelle protection.



Un lien direct vers les logs de ce module est disponible, en bas du menu.

12.2.1 Mise à jour du pare-feu réactif

L'interface de mise à jour du pare-feu réactif propose deux champs de saisie de texte pour spécifier l'adresse du serveur de mise à jour ainsi que le port d'écoute du service de mise à jour, un serveur de mise à jour ainsi qu'un port seront prédéfinis avec des valeurs par défaut. L'interface présente aussi une liste déroulante pour configurer les fréquences de mise à jour. Un bouton "rechercher" permet de lancer une mise à jour manuelle des protections.



Il y a plusieurs fréquence possible, d'où le choix de la liste déroulante, qui seront de 3 fois par jour à 3 fois par semaine.

	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

Menu Communication sécurisée

L'interface de paramétrage du module de communication sécurisée permet d'ajouter de nouveau tunnel et de lister ceux déjà configurés. Il est possible de les supprimer en activant leurs checkbox correspondantes, et en cliquant sur le bouton "supprimer la sélection".



Un lien direct vers les logs de ce module est disponible, en bas du menu.

12.3 Ajout d'une communication sécurisée par tunnel

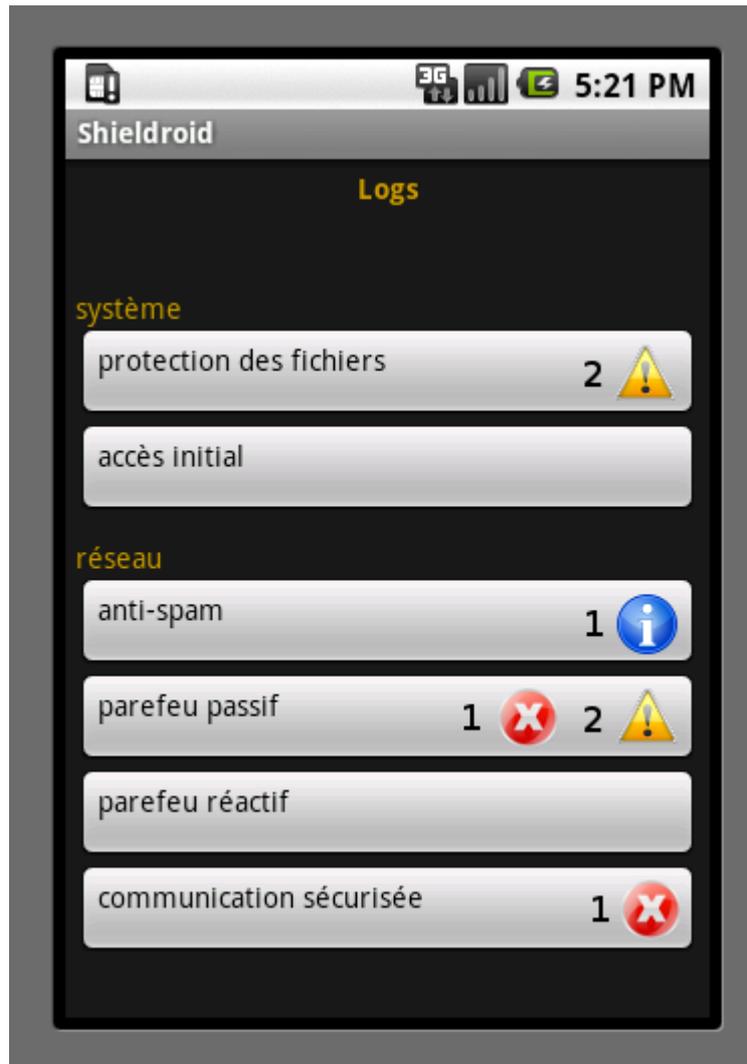
Lorsque l'administrateur demande l'ajout d'un nouveau tunnel, il tombe sur une interface qui lui demande le nom du tunnel et l'adresse IP du point distant sous forme de zone de saisi. Il peut également spécifier le niveau de chiffrement (en fonction de la taille de clé de chiffrement) qui sera négocié lors de l'établissement du tunnel.





13 Menu Logs (Journaux)

Le menu de logs reprend l'ensemble des modules du système Shieldroid sous formes de boutons liens. Ils indiquent, pour chacun, le type et le nombre de nouvelles informations journalisées. Elles sont classées par gravité, avec les plus importantes en premier.



14 Notification pour les journaux

Lorsqu'un problème intervient sur le système, une notification est levée, le système propose 3 niveaux d'authentification. Nous avons ici un exemple d'interface pour chaque niveau de notification :

- Erreur grave : Par exemple un fichier est corrompu au niveau de son intégrité.



- Information : Par exemple une activation du contrôle d'intégrité sur un répertoire.



	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

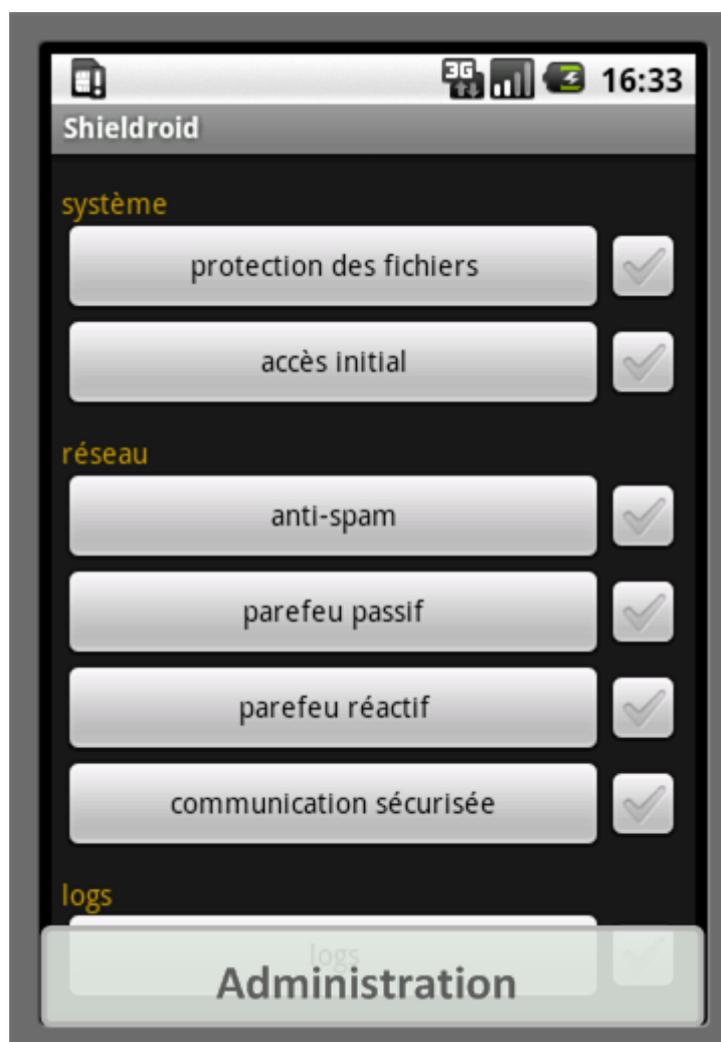
- Avertissement : Par exemple lorsqu'un répertoire sous contrôle n'est plus présent sur le système.



15 Menu paramétrage

Le module de paramétrage permet d'accéder aux données d'informations de l'administrateur.

Afin d'accéder à ce menu, les terminaux qui possèdent la plateforme Android, ont tous une touche "Menu". Cette touche "Menu" servira à afficher le bouton "Administration" avec laquelle on accède à l'interface de paramétrage.



On accède donc à l'interface de paramétrage ci-dessous.



Ce menu permet d'administrer le système Shieldroid. Il permet de changer le mot de passe de l'administrateur, de choisir un algorithme de chiffrement parmi :

- AES,
- DES,
- 3DES,
- Blowfish

Nous pouvons aussi choisir un algorithme d'empreinte numérique :

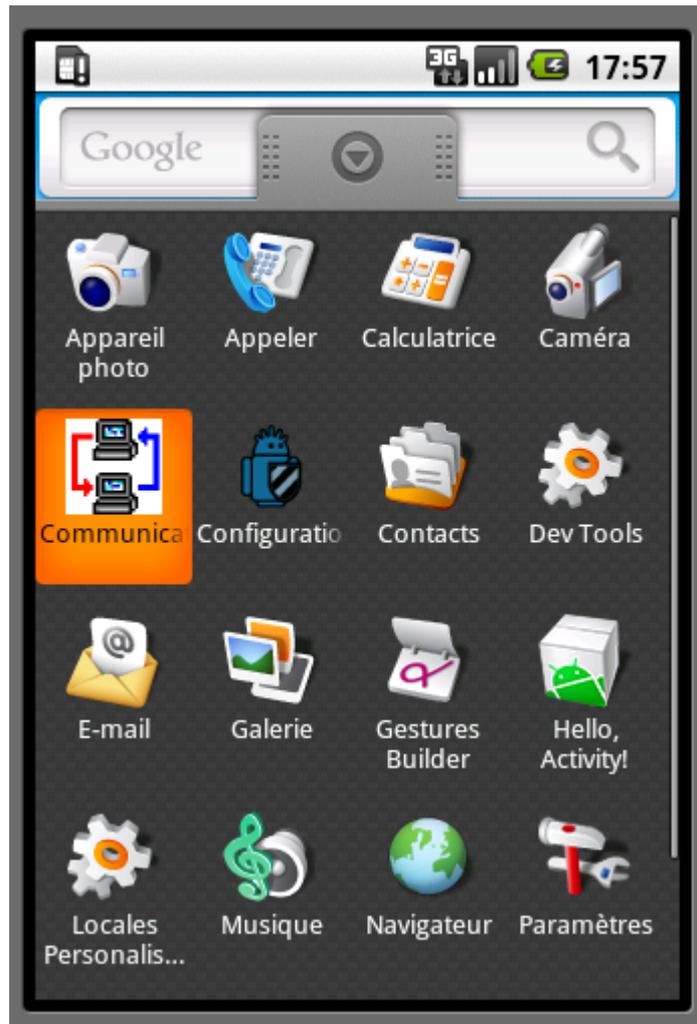
- MD5,
- SHA1,
- SHA256

L'utilisateur peut également forcer la langue de l'application. Lors de la sélection des algorithmes, les valeurs par défaut optimisées pour l'architecture du portable seront proposées, si l'utilisateur modifie ces valeurs, une notification avertira l'utilisateur de l'impact sur le système et la batterie.

	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

16 Icône d'accès à la communication sécurisée utilisateur

Au même titre que les différentes applications que l'on installe sur le système Android, Nous intégrons par défaut l'application communication sécurisée pour l'utilisateur. L'accès se fait en cliquant sur cette icône.



17 Menu Communication Sécurisé pour utilisateur

La vue utilisateur du module de communication sécurisée permet à un utilisateur non authentifié sur le système Shieldroid d'envoyer des fichiers et d'activer des tunnels préconfigurés. Dans le mode tunnel, l'interface propose une liste déroulante des tunnels disponibles afin qu'il puisse en activer un. Dans le mode simple, l'interface demande, sous forme de zone de saisi, l'adresse de l'hôte distant ainsi que le port sur lequel l'hôte distante écoute. Elle propose ensuite un explorateur pour sélectionner le fichier à envoyer.



	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

18 Conclusion

Ce cahier des charges graphique a décrit les différentes applications, en expliquant au client l'utilité des différentes fonctionnalités afin de lui donner une vision plus précise de l'application. Le client pourra s'il le souhaite adapter ou faire modifier certains points suivant ces besoins, avant le début du développement.

Toutes les captures d'écran ne sont pas contractuelles, elles peuvent être amenées à être légèrement modifiées. Cependant si elles sont modifiées, ce sera uniquement pour corriger un oubli, ou une petite erreur. Nous nous engageons à suivre au maximum la solution proposée.

	Projet de Génie Logiciel « Shieldroid »	TD2K
---	--	------

19 Annexes



19.1 Vue globale

