

Projet Zoltan

Cahier des charges

Année 2003-2004

Promotion	INSIA SPE (P2007)
Nom de l'équipe	KilKenny Team
Nom du produit	Zotan
Catégorie	Utilitaire pour Internet
Langage de développement	C++
Site WEB	http://kilkennyteam.free.fr

Créé le	jeudi 18 octobre 2003
Révision n°	1.2
Dernière mise à jour	dddd d mars yyyy
Auteur	KilkennyTeam
Nombre de pages	9

Table des Matières :

1L'ÉQUIPE KILKENNY.....	3
ZELKO GUILLAUME (GHORGHOR).....	3
BRET STEEVY (DARKBAMBI).....	3
TALPAERT CÉDRIC (RANTANPLAN).....	3
NGAN VALERY (IGOR).....	3
LE PROJET.....	4
DESCRIPTIF RAPIDE.....	4
ORIGINES.....	4
CIRCONSCRIPTION.....	4
DESCRIPTIF DÉTAILLÉ.....	4
<i>Principe</i>	4
<i>Fonctionnement</i>	4
1Le serveur principal.....	5
2Le Client.....	5
3Protocoles utilisés.....	5
4Fenêtre principale.....	6
5Chat.....	6
6Droits (fichiers partages).....	6
7Cryptage.....	7
8Environnement de travail partage.....	7
PLANNING PRÉVISIONNEL.....	8
PREMIÈRE SOUTENANCE (19/20 FÉVRIER 2004).....	8
DEUXIÈME SOUTENANCE (14/16 AVRIL 2004).....	8
TROISIÈME ET DERNIÈRE SOUTENANCE (23/25 JUIN 2004).....	8
RÉPARTITION DES TACHES.....	9
GUILLAUME ZELKO.....	9
STEEVY BRET.....	9
CEDRIC TALPAERT.....	9
VALERY NGAN.....	9

1 L'équipe Kilkenny

ZELKO Guillaume (Ghorghor)

- Ne le 10/07/1984 Gisors.

-Obtention du bac S en 2002.

J'ai eu envie de faire ce projet essentiellement basé sur le réseau et les télécoms car ayant codé la partie réseau du projet de l'année dernière j'avais envie de continuer dans ce domaine qui me plaît. De plus le concept du projet est assez intéressant puisque celui-ci constituera un mélange entre un P2P et un Messenger ce qui nous permettra de toucher à de nombreuses parties différentes du réseau.

BRET Steevy (DarkBambi)

-Ne le 15/06/1982

-bac S en 2002.

Ce projet est très intéressant car il va me permettre de travailler dans le domaine du réseau, que je n'ai pas eu l'occasion de travailler l'année dernière. De plus ce projet peut apporter des améliorations par rapport à certains logiciels existants.

TALPAERT Cédric (Rantanplan)

-Ne le 19/06/1982 St-Raphael

-bac STI en 2002.

Je voudrais apprendre à gérer une communication entre 2 ordinateurs distants. Ainsi que l'échange et le chiffrement des données. Car ce sont des domaines qui m'intéressent et que je n'ai pas encore eu l'occasion d'approfondir.

NGAN Valery (Igor)

-Ne le 14/05/1982 Hong Kong

-Bac STI en 2002 Rueil-Malmaison

J'ai toujours été intéressé par les réseaux, et ce projet me permettrait d'approfondir mes connaissances dans ce domaine. Je suis motivé pour développer ce projet en équipe car cela a été une bonne expérience que j'ai eue l'année dernière. Ce projet me permettra de plonger dans le domaine de la sécurité et plus particulièrement dans les échanges de données sur internet.

Le Projet

Descriptif rapide

Le logiciel que nous allons réaliser a travers notre projet a pour but principal l'échange de données entre deux Pc via Internet. Sa structure sera un mélange de P2P et de Ftp, ce qui permettra l'échange de dossiers de tailles importantes entre un groupe d'utilisateurs, avec une fonction chat.

On pourra donc avec ce logiciel échanger des fichiers volumineux avec la simplicité et la sécurité d'un mail chiffré ce que les logiciels déjà existants ne permettent pas. Les axes majeurs de développement de notre projet seront: le découpage de fichiers, la sécurité, le réseau ainsi que la gestion d'une base de donnée.

Origines

La frustration de ne pas pouvoir s'échanger de volumineux fichiers simplement et rapidement via MSN, reprendre un téléchargement, de crypter le contenu des échanges, nous a mené à imaginer ce projet.

Circonscription

La priorité sera de discuter et d'échanger des fichiers sur le net, viendra ensuite la gestion des IP des utilisateurs par un serveur extérieur présent sur le net, on aimerait également garantir la sécurité, la rapidité, et la simplicité pour ses utilisateurs. Finalement si les délais sont suffisants nous pourrions ajouter un plan de travail multi utilisateurs.

Descriptif détaillé

Principe

L'objet principal de notre projet sera le téléchargement et la distribution de données, le partage de fichiers sur un environnement de travail avec d'autres utilisateurs sur internet.

Pour se faire nous mettrons en place une sorte de chat (Messenger) sur lequel on peut s'échanger des données qui ont une capacité importante (>20Mb), contenu dans un répertoire.

Fonctionnement.

Notre projet est constituée de deux grandes parties : une Client et une Serveur.

1 Le serveur principal

Ce serveur sera au cœur de la gestion des différents utilisateurs.

- Il sera actif en permanence sur Internet.
- Il va être utilisé pour gérer les IP lors des différents échanges de données.
- Il servira à stocker tous les login correspondant chacun à une adresse IP Client.
- Il n'y aura que les membres de la team qui pourront le configurer.
- La liste des contacts des utilisateurs sera sauvegardée en cas de réinstallation du logiciel.
- Il ne sera pas utilisé comme intermédiaire lors de l'échange des fichiers.
- Il sera utilisé comme intermédiaire lors d'envoi de messages.

2 Le Client.

Le projet sera surtout porté sur l'application client, qui sera chargée de gérer les tâches suivantes, en ce qui concerne les paramètres entrés par l'utilisateur :

- Son login, et son mot de passe.
- Ses amis, et les fichiers qu'il met à leur disposition (chaque ami n'a pas forcément accès aux mêmes fichiers).

Les fonctions internes au programme :

- Lire l'adresse IP de la machine.
- Gérer/découper les fichiers partagés.
- S'authentifier auprès du serveur principal sur Internet, et récupérer les adresses IP de ses amis.
- Se connecter au pc des autres utilisateurs (selon les droits) grâce à l'ip récupérée sur le serveur.
- Sécuriser tous les échanges, ou simplement l'authentification sur le net. (à paramétrer dans le logiciel)
- Télécharger à partir de plusieurs pc si le même fichier y est partagé.
- Le Client sera à la fois client et serveur, c'est-à-dire qu'il pourra envoyer des données et les recevoir (les données ne seront pas envoyées en sens unique)
- Si le client partage des fichiers, il faudra qu'il ouvre son port sur son pare-feu internet. (s'il en a un).

3 Protocoles utilisés

Le protocole TCP sera utilisé pour le chat
L'UDP pour l'échange de fichier

4 Fenêtre principale

- Quand le client se connectera pour la première fois, le logiciel lancera l'assistant de configuration automatique du logiciel.

Le logiciel s'enregistrera sur le serveur principal. L'authentification de fera par l'intermédiaire d'un login/password.

L'utilisateur pourra enregistrer son password et son login sur son disque dur.

Si le login et le password sont correctes alors une session sera ouverte. (Affichage du type Messagerie instantanée).

-Une fois accepte par le serveur le logiciel mettra l'utilisateur en relation avec les clients inscrits dans son groupe.

-L'utilisateur pourra envoyer des fichier sans limite de taille et pourra interrompre le téléchargement et de le reprendre par le suite.

Il pourra connaître a tout instant l'évolution des transfert qu'il est entrain d'effectuer.

(Nom du fichier, pourcentage termine, et vitesse de transfert)

-Le Client aura la possibilité d'envoyer des fichiers a condition d'avoir les droits d'envoi.

-Lors des échanges classiques c'est l'utilisateur qui va chercher le fichier désire, sur l'un des membres de son groupe. Mais l'utilisateur pourra aussi envoyer des fichiers à ses amis avec leur permission.

Ces fichiers seront envoyés dans un répertoire défini au préalable par le destinataire. Le destinataire pourra définir les options de ce répertoire comme sa taille limite et les droits (lecture/écriture). Si le volume maxi du contenu du répertoire est atteint, la transmission sera suspendue et un message d'erreur sera affiche sur le pc de l'expéditeur et du destinataire.

5 Chat

Le chat permettra de dialoguer soit avec une personne en particulier, soit avec un groupe et dans la même fenêtre.

6 Droits (fichiers partages)

Les droits seront enregistres dans une base de donnée appartenant au projet, ce ne seront pas ceux du système de fichier (sur UNIX ou Windows XP). Ce seront les mêmes pour les fichiers et pour les répertoires. Il n' y aura que les droits de lecture (pas de droit en écriture, ni en exécution).

Chaque personne aura ses propres droits, définit lors de son ajout dans la liste d'amis.

L'utilisateur pourra définir sur son disque dur un répertoire 'morphale', ou les 'amis' pourront déposer des fichiers (ce répertoire n'est pas obligatoire, il pourra être différent pour chaque personne).

7 Cryptage

Toutes les données échangées entre le client et le serveur seront cryptées.

En revanche les échanges entre clients pourront être cryptées ou en clair selon le choix de l'utilisateur. Cette partie devrait occuper une part importante dans le développement du projet car c'est quelque chose de complètement nouveau pour nous, et vu que des failles sont découvertes quotidiennement dans les logiciels les plus célèbres, et les plus utilisés autour de nous, il nous semble que de réaliser un logiciel sans faille ne doit pas être aisé. D'autant plus qu'il faudra éviter d'utiliser 100 % des ressources du processeur afin de chiffrer les données. C'est pourquoi nous devrions utiliser une clé symétrique pour favoriser la vitesse de cryptage/décryptage des fichiers. Cependant pour s'envoyer la clé symétrique sans que celle-ci ne puisse être lue par un tiers, on utilisera une clé asymétrique. Nous ne savons pas aujourd'hui quels algorithmes nous utiliserons, que ce soit pour le hashage, ou pour générer une clé symétrique. Nous les aurons déterminés pour la seconde soutenance.

8 Environnement de travail partagé

Il sera possible de créer un groupe d'amis spécialement pour partager des travaux.

Ces travaux (ou fichiers) seront stockés sur le disque dur de son propriétaire dans un répertoire spécial. Et lorsque un de ces fichiers sera rajouter ou modifier au sein de se répertoire, un message sera envoyé aux autres membres afin de les informer, et seront stockes dans un historique chez chaque membres du groupe.

Planning Prévisionnel

Première soutenance (19/20 février 2004)

Rassembler des documents relatifs à la création d'un serveur et d'un client, ainsi qu'au découpage des fichiers.

Connexion directe entre 2 pc, sans passer par le serveur, la connexion se fera en entrant l'adresse IP.

Le but est de pouvoir utiliser le chat, et de s'envoyer des petits fichiers, en clair.

Si le temps nous le permet, nous commencerons à travailler sur le serveur. Phase de réflexion, et éventuellement début de son développement, en revanche nous pourrons déjà présenter lors de la soutenance un rapport des difficultés rencontrées.

Deuxième soutenance (14/16 avril 2004)

Rassembler des documents sur le cryptage des données. Déterminer les algorithmes de cryptages les mieux adaptés à notre projet.

La connexion se fera en clair par l'intermédiaire du serveur, la partie client gèrera la liste d'amis, ainsi que les droits. Le client gèrera l'interruption du téléchargement et sa reprise, grâce au découpage des fichiers.

Troisième et dernière soutenance (23/25 juin 2004)

Tous les échanges seront cryptés (identification auprès du serveur, et transfert de fichiers client-client), le client gèrera également l'espace de travail. Le logiciel devra être opérationnel.

Répartition des taches

Guillaume Zelko

Chat
Mise en place du serveur
GUI
Environnement de travail partage

Steevy Bret

Découpage des fichiers
GUI
Cryptage des données

Cedric Talpaert

Procédure d'authentification entre le client et le serveur
Gestion de la liste d'amis et des droits.
Mise en place du serveur
Site Web

Valery Ngan

Mise en place du serveur
Procédure d'authentification entre le client et le serveur
Cryptage des données
Environnement de travail partage