Goatsoft Corporation présente :

GLOSTER©

Cahier des charges

Par les créateurs de Tuxout :

Guillaume "CrYpToNyM" MOISSAING (moissa_g)
François "Meteoryte" GOUDAL (goudal_f)
Freddy "Loki" SARRAGALLET (sarrag_f)
Guillaume "Z" LAZZARA (lazzar_g)

Novembre 2004

Bitou@InfoSpe-Promo2008

"Où que nous mène la baisse de confiance qui nous occupe, il est nécessaire d'imaginer toutes les voies de bon sens" (un visionnaire)

Table des matières

1 Introduction

Après avoir survécu à la Sup, l'équipe des quadricolor change de nom et revient pour une nouvelle aventure...

Comme d'habitude, le projet fait parti des choses que nous attendons le plus. Il est l'occasion pour nous d'appliquer toute la partie théorie de notre apprentissage. Il l'est d'autant plus pour nous cette année car nous avons un vrai choix de la plateforme et du langage.

Finis le Delphi et OpenGl. Fini tout ce qui concerne le réseau... Oups ! Non en fait, ça on garde ! Cette année nous allons donc découvrir les joies du C/C++ (surtout le C++ en fait) et des systèmes linux ! Le projet devant être à tout prix une application, il sera aussi plus facile d'utiliser des algorithmes déjà vus en cours.

Cette année nous avons donc choisi de développer un logiciel de Peer-to-Peer. Encore un me direz-vous ? Oui, mais ça ne sera pas n'importe lequel puisque... ce sera le notre ! Plus sérieusement, contrairement à la plupart des logiciels de P2P, le notre sera crypté et sera plutôt réservé à une petite communauté.

Du fait de la baisse de confiance contemporaine, il est nécessaire d'étudier la somme des problématiques de bon sens. C'est pourquoi, comme l'année dernière, nous découperons notre projet en plusieurs parties afin de mieux répartir les tâches. Mais avant commençons par donner un point de vue globale du projet...

2 Origine et nature du projet

Cette année, l'équipe a été rapidement constituée dans la mesure où l'année dernière tout s'était parfaitement bien passé. Le nom de groupe a été changé, cependant ce n'est pas pour refléter un changement déquipe comme je viens de l'expliquer. C'est uniquemet suite à un "delire" un peu particulier... Pour des raisons évidentes de protection de nos lecteurs contre des contenus choquants (voire affligeants...), nous ne pourrons dévoiler ici notre source d'inspiration.
Après cette petite anecdote inutile, qui a quand même eu le mérite de remplir la moitié de la page, passons aux choses sérieuses.

Pour comprendre aujourd'hui pourquoi GoatSoft Corporation a décidé de développer un logiciel de peer-to-peer, il est nécessaire de vous remettre dans le contexte (attention, pour une immersion totale, il est conseillé de lire ce qui va suivre avec le thème de Star Wars en musique de fond) :

"Au cours du XX$^{\text{ème}}$ siècle après J.C., une poignée d'informaticiens réussit à relier plusieurs ordinateurs entre eux. Pour la première fois, il était possible d'échanger des données entre deux machines. Ce fut une révolution technologique, certains voyaient déjà des applications multiples et pensaient que cela aurait une utilité foudroyante dans notre vie de tous les jours. L'exemple le plus frappant fut celui de placer une webcam prés d'une machine à café pour surveiller le niveau de café restant. Suite à cette démonstration époustouflante, l'Internet se développa.

Au fur et à mesure que cet outil se popularisait, les vitesses de transmission et donc les possibilités d'exploitation augmentaient. On vit donc apparaître au début du XXI$^{\text{ème}}$ siècle, une nouvelle utilité pour l'Internet : l'échange de fichiers ou peer-to-peer. Chacun se mettait à partager ses fichiers aussi bien copyrightés que libres de droit. Le peer-to-peer est donc devenu incontournable et un support de 1$^{\text{er}}$ choix pour la diffusion de logiciels libres. Tout se passait donc pour le mieux dans le meilleur des mondes : le monde virtuel.

Mais au fin fond du monde réel, une faction anti peer-to-peer grandissait dangereusement et commençait à persécuter les utilisateurs de peer-to-peer.

Pour faire face à cette faction oppressive, les utilisateurs mirent en place une résistance. Elle se matérialisa sous différentes formes : changement de protocol, partage décentralisé...Seulement tout ceci ne suffisait pas et aujourd'hui seul un logiciel capable de crypter des données serait à la hauteur pour permettre aux utilisateurs de continuer à échanger des fichiers en tout tranquilité..."

C'est pourquoi, GoatSoft Corporation a jugé utile de développer cette année, pour le plus grand bonheur d'entre vous, un logiciel de peer-to-peer crypté, j'ai nommé Gloster.

Vous l'avez maintenant compris, Gloster ne sera pas un client de peer-to-peer comme les autres. Ce logiciel permettera de créer des petites communautés. Chaque utilisateur sera authentifier par une clé privé et une clé publique. Tous les échanges de données seront cryptés. Les utilisateurs auront accès à la liste des utilisateurs et pourront chatter avec eux. Enfin, Pour optimiser le transfert de fichier, nous utiliseront aussi la compression de données qui nous obligerons à effectuer es contrôles d'intégrités.

3 Objet de l'étude

3.1 Réseau

Un logiciel de peer-to-peer sans réseau risque de très mal fonctionner, c'est pourquoi cette tâche est l'une des plus importantes pour ce projet. Il faut de plus tenir compte du fait qu'il n'y a pas de serveur, ce qui rend beaucoup difficile la mise en relation des différents membres du réseau.

3.1.1 Protocole

Le protocole devra gérer tout le dialogue entre les clients afin de prendre en compte différentes actions, telles que demande d'un fichier et transfert de fichier, demande de la liste des fichiers partagés, chat, échanges de clés de session, etc... Il devra prendre en compte la gestion de clients passifs (sur lesquels on ne peut pas initier de connexion directe).

3.1.2 Strcture du Réseau (graphe)

Le réseau sera formé de plusieurs clients qui seront reliés entre eux par des connexions TCP, cependant tout le monde ne sera pas connecté sur tout le monde, il faudra donc établir un graphe qui représentera les liens entre les clients ainsi que des algorithmes de détermination de plus court chemin afin de déterminer la route à faire suivre à un paquet pour rejoindre un client à partir d'un autre.

3.1.3 Broadcast

Certaines informations devront être diffusées à tous les clients sans exception, comme par exemple pour signaler à tout le monde l'arrivée d'une nouvelle personne sur le réseau. Il faudra donc prévoir des fonctions de broadcast qui consisteront a parcourir le graphe qui représente le réseau.

3.2 Interface

Nous aurions très bien pu faire une application console qui afficherait un prompt dans lequel on aurait pu taper des dizaines de commandes munies de 50 paramètres chacune, cependant nous nous sommes dit que ca ne serait pas "User Friendly". C'est pourquoi nous avons décidé de developper plusieurs interfaces permettant ainsi de manipuler le logiciel de differentes manières.

3.2.1 GUI

Gloster s'adresse à tout type de public, il doit donc être simple et agréable à utiliser, pour cela une GUI s'impose. Celle-ci sera développée avec la librairie Qt qui a pour avantage d'être disponible sur de nombreuses plateformes tel que Windows, Linux/Unix, MacOS...

3.2.2 Administration distante

Gloster doit être simple à utiliser, cela ne doit cependant pas le limiter sur le plan fonctionnalités. Pour les utilisateurs un peu plus avancés, il y aura donc moyen de piloter Gloster à distance afin de pouvoir par exemple lancer des téléchargements sur son PC familial depuis le bureau, pendant la pause café bien sûr.

3.3 Cryptage

Hormis le fait que les réseaux Gloster seront dépourvus de serveurs, ils seront également cryptés afin de garantir la confidentialité des donnés y circulant. De plus, les réseaux seront privés, c'est à dire que nimporte qui ne rejoint pas nimporte quel réseau.

3.3.1 Authentification

L'accès à un réseau se déroulera en plusieurs étapes, tout d'abord avec une clé pour le réseau qui sera cryptée par un algorithme de cryptage symétrique, par la suite, l'utilisateur devra également s'authentifier via un système d'algorithme à clé privée/clé publique.

3.3.2 Cryptage des données

Pour le cryptage des données, chaque utilisateur devra posséder la clé publique de tous les autres, les échanges de clés étant gérés par le protocole. Ainsi, lorsqu'un client doit envoyer un fichier à un autre, il crypte le contenu du fichier grâce à la clé publique de la personne pour qui ce fichier est destiné, ainsi seule le destinataire du paquet pourra décrypter le fichier. Donc ce dernier peut très bien transiter par d'autres clients intermédiaires si besoin, cela ne gène pas la confidentialité.

3.4 Transferts de fichiers

Pour les transferts de fichiers, ceux-ci seront découpés en petits morceaux. Ainsi, il sera possible de gérer le multi-sourcing, en effet, on pourra trés bien télécharger un morceau d'un fichier sur un client et un autre morceau sur un autre client si celui possède aussi le fichier, ce qui permettra de télécharger plus rapidement.

3.4.1 Compression

Afin d'économiser de la bande passante, les données transférées seront compressées à l'aide d'un algorithme de compression sans perte. Celui-ci devra être suffisament rapide pour que le temps de compression soit le plus court possible afin que cette operation soit le plus transparente possible pour l'utilisateur, tout en faisant gagner du temps sur un transfert de fichier.

3.4.2 Contrôle d'integrité

Afin de s'assurer qu'un fichier transféré est parfaitement identique à l'original, et aussi pour verifier si un fichier présent sur deux sources differentes est le même, il sera effectué un contrôle d'intégrité à partir d'un Hash généré à partir du fichier. Cela permet de s'assurer que le fichier reçu est correct et de pouvoir assurer un multi-sourcing correct.

3.5 Aide en ligne

Bien entendu, le logiciel sera pourvu d'une aide en ligne pour pouvoir prendre en main le logiciel très facilement.

3.6 Installeur

Gloster sera aussi fourni avec un installeur permettant de l'installer et le désinstaller très facilement. Il sera également distribué sous forme de packages pour les systèmes qui le gèrent (Deb, RPM, etc...)

3.7 Site Web

Un site Web permettra de suivre l'évolution du développement, d'avoir des retours d'utilisateurs sur des éventuels problèmes ou bugs qu'ils auraient rencontrés. Il donnera aussi accès à un CVS afin de donner accès au code source en permanence et ce, avec les versions les plus récentes.

4 Technologie et méthodologie

4.1 Le matériel

	CrYpToNyM	Loki	Meteoryte	Z
Processeur	A64 3000+	P4 3Ghz	Centrino 2ghz	P4 3ghz
RAM	512 DDR	512 DDR	1024 DDR	1024 DDR

4.2 Le budget

* Windows (XP et 2000)	**0 .00** € (license EPITA)
* GNU/Linux	**0 .00** €
* The GIMP	**0 .00** €
* GDB	**0 .00** €
* Qt Designer	**0 .00** € (pour un utilisation non commerciale)
* Notre reflexion	Variable selon l'individu
* La vie d'un arbre (papier)	ça n'a pas de prix !
* Boissons (café essentiellement)	Beaucoup !

Le developpement se faisant avec essentiellement gráce a des outils libres, le coût est infime (bien suî, en ne considerant que le coût materiel, car la quantité de papier et les litres de boissons necessaires a notre survie durant les coding nights sont loin d'être negligeables...).

5 Répartition des tâches

Légende

Niveau d'avancement/priorité
– : ébauche
\+ : avancé
* : terminé

5.1 Première Soutenance

	CrYpToNyM	Loki	Meteoryte	Z
Reseau	–		–	–
Interface		–		
Cryptage				
Compression				
ContrÔle d'intégrité				
Aide et CD				
Installeur				
Site Web				

5.2 Deuxième Soutenance

	CrYpToNyM	Loki	Meteoryte	Z
Reseau	+		+	+
Interface		+		
Cryptage				
Transfert de fichiers				
Aide et CD				
Installeur				
Site Web	–			–

5.3 Troisième Soutenance

	CrYpToNyM	Loki	Meteoryte	Z
Reseau	*		*	*
Interface		*		
Cryptage		–	–	
Transfert de fichiers	–	–		–
Aide et CD				
Installeur				
Site Web	+			+

5.4 Quatrième Soutenance

	CrYpToNyM	Loki	Meteoryte	Z
Reseau	*		*	*
Interface		*		
Cryptage		*	*	
Transfert de fichiers	*	*		*
Aide et CD	*	*	*	*
Installeur		*		
Site Web	*			*

6 Conclusion

Vous l'aurez compris, GoatSoft Corporation est donc sur le point de développer un logiciel de peer-to-peer révolutionnaire. A la fois sécurisé et multi plateforme, Gloster répondra à toutes vos attentes en terme de besoin pour les transferts de fichiers.

Et surtout n'oubliez pas : quelle que soit l'inertie qui nous occupe et considérant la conjoncture de la société, il est nécessaire de ne pas négliger toutes les alternatives possibles. Gloster en fait partie, alors pensez y.