S^3 - Safe Security System

Bellone Sylvain - Mao Julien - Mérault Dimitri - Taront Vincent

Novembre 2004

Table des matières

1 Introduction **3**

2 Origine et nature du projet **4**
2.1 Le groupe 4
2.2 Le logiciel 4

3 Objet de l'étude **5**
3.1 Le but 5
3.2 Les intérêts 5

4 Structure du projet **6**
4.1 Fonctionnel 6
4.1.1 Le chiffrement 6
4.1.2 La compression 6
4.1.3 La stéganographie 6
4.1.4 L'interface 6
4.1.5 Tâches annexes au projet 7
4.2 Technologique et méthodologique 8
4.2.1 Moyens matériel 8
4.2.2 Moyens logiciel 8
4.3 Opérationnel 8

5 Planning **9**

6 Conclusion **10**

1 Introduction

Dans ce cahier des charges, nous allons vous présenter S^3 (Safe Security System), un logiciel de sécurité comprenant trois fonctionnalités principales : de chiffrement, de compression et de stéganographie.
Au cours de ce cahier vous seront détaillés l'intérêt du projet, sa structure (les aspects fonctionnel, technologique et méthodologique ainsi qu'opérationnel).
Finalement un planning sera fournit vous permettant de distinguer la répartition des tâches au sein du groupe ainsi que les échéances de ces différentes tâches.

2 Origine et nature du projet

Tout d'abord nous voulions faire un logiciel comprenant une partie réseau, comme un client IRC. Mais nous nous sommes très vite aperçu des limites d'un tel projet et de son manque d'originalité. C'est pourquoi nous nous sommes orienté vers le domaine de la sécurité. Plusieurs idées nous sont venues, notamment la stéganographie. Mais pour présenter un projet plus complet nous avons choisi de rajouter plusieurs fonctionnalités : chiffrement et compression. Ainsi est né S^3 (Safe Security System).

2.1 Le groupe

Le groupe est composé de 4 élèves d'Info-Spé de l'EPITA :
- Bellone Sylvain
- Mao Julien
- Mérault Dimitri
- Taront Vincent

2.2 Le logiciel

S^3 (Safe Security System) est un logiciel offrant à la fois des possibilités de cryptage de données, de compression de fichiers et il permet également de cacher un document à l'intérieur d'une image.

L'utilisateur aura la possibilité de crypter du texte en important dans le logiciel des fichiers aux formats : Word (.doc), OpenOffice (.sxw), bloc-note (.txt) ou document texte créés à l'aide d'un éditeur comme Emacs.

Il aura alors la possibilité de crypter ses données avec 3 niveaux de cryptage différents :
- niveau normal (ou encore bas niveau)
- niveau plus élevé
- niveau maximal (ou haut niveau)

Une fois le document déchiffré, l'utilisateur obtiendra un fichier au format LaTeX(.tex).

3 Objet de l'étude

3.1 Le but

Ce projet est l'une des choses majeures de cette année. Le but final est, à la fin de l'année, de fournir une application fonctionnelle, facilement exploitable et sans bugs. Cela va nous permettre d'apprendre beaucoup au cours de sa réalisation. Tout d'abord, il s'agit d'un projet de presque 6 mois, ce qui va nous obliger à travailler régulièrement tout au long de l'année. Ensuite, ce projet doit être réalisé en groupe de quatres personnes, ce qui nous initie au travail de groupe sur une longue durée.

3.2 Les intérêts

La durée de ce projet fait de lui une bonne initiation pour plus tard, car il est possible qu'un jour nous devions travailler sur des projets encore plus longs. C'est donc un très bon exercice pour chacun.

De plus, ce projet se faisant par groupe de 4, cela va nous obliger à nous réunir régulièrement, à bien organiser le travail de chacun afin que le projet avance de manière régulière. Là encore, cette initiation au travail en groupe (et de plus sur une longue durée) est vraiment importante pour le futur, car il est important au sein d'une entreprise ou d'une équipe que tout le monde soit bien organisé afin de fournir un travail de qualité. Si un membre du groupe rencontre un problème, il peux rapidement demander de l'aide aux autres, et de cette manière, on apprend beaucoup plus vite et c'est très agréable. En plus de cette formation pour le futur, ce projet va également nous permettre de nous plonger en profondeur dans un domaine qui nous intéresse particulièrement puisqu'il s'agit d'un projet relativement libre. Nous allons donc pouvoir travailler de manière assez poussée dans un domaine qui nous plaît et en développer une application.

C'est donc une très bonne expérience, que ce soit pour l'apprentissage du travail de groupe, mais aussi pour le travail personnel, car pour ne pas ralentir le groupe, chacun doit y mettre du sien et cela motive donc beaucoup plus que dans le cadre d'un projet personnel.

4 Structure du projet

4.1 Fonctionnel

4.1.1 Le chiffrement

Le premier but de Safe Security System est de créer un logiciel qui soit capable de crypter du texte. Pour réaliser ceci nous utiliserons l'algorithme Rijndael (prononcé "Raindal") plus communément appelé AES pour Advanced Encryption Standard.

Pourquoi avoir choisi cet algorithme ?

AES est L'algorithme de chiffrement destiné à remplacer DES (Data Encryption Standard) qui est devenu trop faible au regard des attaques actuelles.

AES suit les spécifications suivantes :
- L'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet.
- C'est un algorithme de type symétrique (comme le DES).
- C'est un algorithme de chiffrement par blocs (comme le DES).
- Il supporte différentes combinaisons [longueur de clé]-[longueur de bloc] : 128-128, 192-128 et 256-128 bits (en fait, Rijndael supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard).

Pour se faire une idée concrète de la puissance de l'AES actuellement si l'on suppose que l'on puisse construire une machine capable de cracker une clé DES en une seconde (donc qui puisse calculer 255 clés par seconde), alors cela prendrait 149 mille milliards d'années pour cracker une clé AES.

Enfin il sera possible de choisir une clé de cryptage aléatoire ou d'en créer une.

4.1.2 La compression

Après avoir crypté un document, Safe Security System sera capable de compresser le résultat du chiffrement, ou si l'utilisateur ne le souhaite pas de le laisser non compressé.
Nous utiliserons donc une compression sans pertes de données.

4.1.3 La stéganographie

Le principe de la stéganographie est de dissimuler une information dans une autre, pour que cette première passe inaperçue, dans le cadre de notre projet informatique nous dissimulerons un texte préalablement crypté dans une image.

Pour les formats des images nous souhaiterons utiliser des images au format PNG, dont l'algorithme est en open source et également si possible en BMP (mais l'algorithme n'est pas open source).

4.1.4 L'interface

L'interface se doit d'être claire et intuitive. Nous ferons en sorte de ne pas la surcharger. De plus les principales caractéristiques du projet devront être accessibles et exécutables directement dans l'interface principale, à l'aide de boutons. Comme choisir une clé de cryptage, crypter le fichier, décrypter...

Elle sera réalisée soit avec GTK soit avec QT, cela en fonction du choix du langage de programmation retenu : C ou C++.

Safe Security System utilisant une interface graphique, des skins seront fournis avec le programme qui permettront à l'utilisateur de pouvoir changer l'apparence de ce dernier.

4.1.5 Tâches annexes au projet

- Programmation d'un module d'installation et de désinstallation.
- Création d'un site internet qui devra être mis à jour pour chacune des soutenances et où y seront exposées les différentes partie du projet et les péripéties du groupe y seront retranscrites.

4.2 Technologique et méthodologique

4.2.1 Moyens matériel

Membre	Sylvain	Julien	Dimitri	Vincent
CPU	Athlon-64 3000+	Athlon XP 2000+	Pentium M 1,4GHz	Pentium M 1,6Ghz
Mémoire	512Mo	512Mo	512Mo	512Mo
Carte graphique	ATI9600	GeForce4Ti4200	ATI9200	ATI9000Pro
OS	Linux - Debian 3.2			

4.2.2 Moyens logiciel

Durant le développement du logiciel, nous utiliserons les logiciels suivants :
- Linux - Debian
- GCC
- GTK ou QT
- Gimp
- Emacs

4.3 Opérationnel

Le logiciel devra être réalisé en environ six mois et devra être fini et parfaitement opérationnel pour la soutenance finale.

Pour calculer les coûts nécessaire au développement de ce logiciel, il faut ajouter les prix des différents PC mais, aussi la nourriture, les tickets du métropolitain, la location des locaux où nous passerons nos coding parties. Nous arrivons finalement à une somme approchant les 7550 €.

Le logiciel n'étant absolument pas à but lucratif, sa rentabilité sera nulle voir négative au vu des dépenses nécessaires au développement.

5 Planning

Soutenances	1re	2e	3e	4e
Sylvain	Recherche sur les algorithmes utilisés et début de l'implémentation de l'algorithme de chiffrement.	1. Suite de l'implémentation de l'algorithme de chiffrement. 2. Stéganographie dans une image. 3. Début de la conception de l'interface.	1. Suite de l'implémentation de l'algorithme de chiffrement. 2. Stéganographie dans un fichier audio. 3. Conception de skins pour l'interface.	Logiciel fini
Julien	Recherche sur les algorithmes utilisés et début de l'implémentation de l'algorithme de chiffrement.	1. Suite de l'implémentation de l'algorithme de chiffrement. 2. Implémentation des algorithmes de compressions.	1. Suite de l'implémentation de l'algorithme de chiffrement. 2. Importation de fichiers texte et exportation dans un fichier LaTeX.	Logiciel fini
Dimitri	Recherche sur les algorithmes utilisés et début de l'implémentation de l'algorithme de chiffrement.	1. Suite de l'implémentation de l'algorithme de chiffrement. 2. Implémentation des algorithmes de compressions.	1. Suite de l'implémentation de l'algorithme de chiffrement. 2. Importation de fichiers texte et exportation dans un fichier LaTeX.	Logiciel fini
Vincent	1. Recherche sur les algorithmes utilisés et début de l'implémentation de l'algorithme de chiffrement. 2. Début de la conception du site web.	1. Suite de l'implémentation de l'algorithme de chiffrement. 2. Stéganographie dans une image. 3. Suite de la conception du site web.	1. Suite de l'implémentation de l'algorithme de chiffrement. 2. Stéganographie dans un fichier audio. 3. Site web.	Logiciel fini

6 Conclusion

Pour conclure, la réalisation de ce projet nous sera très bénéfique. En effet, nous pourrons mettre en pratique les algorithmes que nous verrons au cours de l'année comme les algorithmes de hachages lors de la compression de donnés. De plus le chiffrement, la compression et la stéganographie sont des domaines qui nous passionnent. Nous nous investirons donc de manière assidue à la réalisation de ce projet et cela nous apportera une grande satisfaction lorsqu'il sera mené à terme.

Les difficultés liées aux principes mathématiques derrières les algorithmes de chiffrement et de compression constituent une véritable barriére, mais cela ne nous fais pas peur.
Etant donné que tous les membres du groupe sont issues de la même classe de sup, nous nous connaissons déjà et le travail de groupe sera présent. Les journées de code ensemble seront très instructives et représenteront pour nous de bons moments à passer.