

Projet PGP

Étude et implantation d'un outil graphique de
gestion de clefs PGP



Rapport de projet

25 mai 2015

Auteur(s):

Pierre BALMELLE,
Lucas BARBAY,
Matthieu FIN,
Ibrahima SORRY BARRY,
Olivier THIBAUT

1 Remerciements

Avant de débiter ce rapport, il nous parait indispensable de remercier les personnes qui ont contribué au bon déroulement de ce projet.

Nous remercions tout d'abord notre cliente, madame Magali BARDET, pour sa participation, son attention et la confiance qu'elle nous a accordé au cours de notre mission.

D'autre part, nos remerciements vont aussi à monsieur Karim ABDELLAH GODARD ainsi que monsieur Rémi DIONISI, pour la formation, le suivi et le soutien qu'ils nous ont apporté au cours de l'année.

Enfin, nous remercions l'ensemble de l'équipe enseignante du département informatique de rouen, pour les connaissances qu'ils nous ont fournis lors de notre formation, sans quoi ce projet n'aurait pas eu lieu.

Table des matières

1	Remerciements	1
2	Introduction	3
2.1	Contexte	3
2.2	L'équipe	3
3	Présentation du projet initial	3
3.1	Objectifs	3
3.2	Fonctionnalités	4
3.3	Contraintes	4
3.4	Organisation	4
4	Présentation du projet final	5
4.1	Objectifs	5
4.2	Organisation	5
4.3	Fonctionnalités	5
5	Les problèmes rencontrés	6
5.1	Problèmes organisationnel	6
5.1.1	Équipe	6
5.1.2	Planning	6
5.2	Problèmes techniques	6
5.2.1	Maîtrise des outils	6
5.2.2	Maîtrise de GnuPG	6
5.2.3	Communication GnuPG	6
6	Bilan du projet	6
6.1	Compétences acquises	6
6.1.1	Technique	6
6.1.2	Organisationnel	6
6.2	Axes d'amélioration	6
6.3	Rétrospective	6
7	Conclusion	6

2 Introduction

Au cours de notre première année de Master Informatique, un projet annuel en équipe nous a été confié afin de mettre en pratique ce qui nous a été enseigné dans l'unité "Gestion de projet". Il s'agit donc d'apprendre à s'organiser en équipe, faire preuve de méthodologie et d'adaptabilité pour mener à bien les objectifs d'un projet informatique. Ce rapport a pour but de présenter nos travaux durant ce projet.

Dans ce cadre, nous avons eu pour client Mme Magali BARDET, enseignante et responsable du Master Sécurité des Systèmes Informatiques (SSI) de l'UFR des Sciences et Techniques de Rouen. Notre mission s'est déroulée du 17 octobre 2014 au 1^{er} mai 2015. Durant cette période, nous avons été formé à la gestion de projet par M. Rémi DIONISI ainsi que M. Karim ABDELLAH GODARD.

2.1 Contexte

Ce projet a été réalisé dans le cadre de la première année du Master Sécurité des Systèmes d'informations enseigné à l'Université de Rouen. Ce projet est découpé en deux parties et a commencé au début de l'année. Il nous a été demandé au premier semestre de rédiger les documents de Gestion de projets qui ont servi de base durant toute la durée du projet. Au second semestre il a fallu développer l'application en s'aidant des documents rédigés et en les faisant évoluer au fur et à mesure du projet.

2.2 L'équipe

L'équipe de ce projet était composée au début de 7 étudiants en première année du master évoqué ci-dessus : Pierre Balmelle, Lucas Barbay, Bertille Bouillie, Mathieu Fin, Guillaume Leroy, Ibrahima Sorry Barry et Olivier Thibault. Nous avons dû réaliser ce projet dans le cadre du module de gestion de projet sous la tutelle de Monsieur Karim ABDELLAH GODARD. et grâce aux cours de Monsieur Rémi DIONISI. Le sujet de ce projet nous a été donné par Magali Bardet, enseignante-chercheuse à l'Université de Rouen.

3 Présentation du projet initial

Pour introduire ce projet, nous allons commencer par parler du standard OpenPGP. Ce standard est un format de cryptographie normalisé dans la RFC 4880. OpenPGP décrit le format des messages qui sont adaptés aux outils permettant l'envoi sécurisés de message ou bien le stockage de message. GnuPG (GNU Privacy Guard) est un de ces outils. Il se base sur le logiciel PGP et utilise un système hybride liant cryptographie symétrique et asymétrique pour permettre l'envoi de message chiffrés et/ou signés. Pour pouvoir s'échanger des messages, les utilisateurs de GPG doivent s'envoyer leur clé publique qui servira au chiffrement des messages.

3.1 Objectifs

L'objectif de ce projet est de développer un outil graphique de gestion de clés PGP. Il existe déjà plusieurs éditeurs permettant d'utiliser GPG graphiquement mais aucun ne permettent une gestion fine des clés et la partie toile de confiance n'est pas intuitive. Il nous est donc demandé de réaliser une interface qui soient plus complète que les outils existants. L'objectif est dans un premier temps d'étudier complètement GnuPG et OpenPGP pour comprendre parfaitement son utilisation et réaliser un logiciel le plus exhaustif possible. L'interface réalisée devra permettre aux utilisateurs de faire des réglages techniques qu'ils soient experts ou novices. Un document expliquant les fonctionnalités devra être livré avec le projet. Enfin il est demandé d'implanter l'attaque sur les KeyID décrite dans le magazine de sécurité informatique le MISC. Cette attaque est basée sur les mauvais usages de PGP par les utilisateurs.

3.2 Fonctionnalités

Les principales fonctionnalités du projet sont :

- Exécution d'actions GPG
Appel des actions via l'interface (création, modification, suppression..)
- Chiffrer / déchiffrer / signer / vérifier
Chiffrer ou déchiffrer ou signer ou vérifier un message copié dans l'éditeur de l'interface. Il est possible d'exporter le résultat dans un fichier ou d'importer un fichier. Dans ce dernier cas, le résultat est affiché via l'interface.
- Affichage des commandes, des retours et des erreurs
L'utilisateur peut choisir d'afficher ou non les commandes, les retours et les erreurs associés à chaque action GPG.
- Choix du profil utilisateur
L'utilisateur peut choisir son profil au lancement de l'interface via l'option -P ou en cours d'utilisation. Si au lancement l'option n'est pas lancée et qu'aucun profil par défaut n'est défini, l'utilisateur doit choisir un profil. Lors de l'installation, un profil par défaut est créé.
- Modification de la toile de confiance
Modification de la toile de confiance par un changement de niveau de confiance, l'ajout d'une nouvelle clé ou la modification d'une clé.
- Calcul d'une seconde pré-image pour une clé donnée
Attaque permettant d'obtenir une nouvelle clé contenant le même KeyId que la première.
L'attaque sur les KeyId est indépendante et ne fera pas partie de l'interface graphique.

3.3 Contraintes

L'application doit fonctionner sur le système d'exploitation GNU/Linux, en particulier sous les environnements KDE et Gnome. La validité et la confiance doit être représentée sur l'interface par différents niveaux de couleurs. L'interface doit être à la fois pédagogique et précise pour faciliter l'utilisation de GPG.

3.4 Organisation

Pour l'organisation de ce projet, il nous a été demandé d'utiliser une méthode agile. Nous avons décidé de choisir scrum avec comme scrum master Olivier, comme chargés client Bertille et Ibrahima, comme architectes Mathieu et Guillaume et enfin Pierre et Lucas comme testeurs. Cette équipe est encadré par le propriétaire du produit Magali BARDET et le consultant en gestion de projet Karim ABDELLAH GODARD.

4 Présentation du projet final

4.1 Objectifs

Pendant le développement du projet, deux membres nous ont quittés (Bertille et Guillaume), ce qui nous a forcé à revoir toute notre planification, n'ayant plus les moyens humains pour tenir le rythme prévu.

4.2 Organisation

Le projet a été replanifié et découpé en deux livraisons. L'attribution des tâches a été refaite, avec la répartition suivante :

- Ibrahima sur l'étude de GPG,
- Lucas sur l'attaque sur les KeyID,
- Les autres (Matthieu, Olivier et Pierre) sur le développement de l'application.

4.3 Fonctionnalités

Les fonctionnalités ayant été complétées sont :

- Exécution d'actions GPG
 - Création, exportation, importations de clés (en local)
- Chiffrer / déchiffrer / signer / vérifier
 - Chiffrer ou déchiffrer ou signer ou vérifier un fichier.
- Affichage des commandes, des retours et des erreurs
 - L'utilisateur peut choisir d'afficher ou non les commandes, les retours et les erreurs associés à chaque action GPG.
- Création / Modification / Suppression du profil utilisateur
- Modification de la toile de confiance
 - Modification de la toile de confiance par un changement de niveau de confiance, l'ajout d'une nouvelle clé ou la modification d'une clé.
- Calcul d'une seconde pré-image pour une clé donnée
 - Attaque permettant d'obtenir une nouvelle clé contenant le même KeyId que la première.

Les fonctionnalités qui ont été supprimées par rapport au plan initial sont :

- Toile de confiance graphique
 - Représentation de la toile de confiance sous forme de graphe
- Chiffrer / déchiffrer / signer / vérifier
 - Chiffrer ou déchiffrer ou signer ou vérifier le texte contenu dans l'éditeur de l'interface.
- Edition de clé
 - Quelques fonctions d'édition de clé ne sont pas implémentées, comme la révocation d'une clé ou la signature avec une clé en particulier
 - La partie interface graphique a été validée par le client, mais malheureusement l'attaque et l'étude sur GPG n'ont pas été validés car ils n'ont pas été rendus à temps.

5 Les problèmes rencontrés

5.1 Problèmes organisationnel

5.1.1 Équipe

5.1.2 Planning

5.2 Problèmes techniques

5.2.1 Maîtrise des outils

5.2.2 Maîtrise de GnuPG

5.2.3 Communication GnuPG

6 Bilan du projet

6.1 Compétences acquises

6.1.1 Technique

6.1.2 Organisationnel

6.2 Axes d'amélioration

6.3 Rétrospective

7 Conclusion