Projet PGP

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

UNIVERSITÉ DE ROUEN

Rapport de projet

26 mai 2015

Auteur(s):
Pierre Balmelle,
Lucas Barbay,
Matthieu Fin,
Ibrahima Sorry Barry,
Olivier Thibault

Remerciements

Avant de débuter ce rapport, il nous paraît 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 suivit 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 connaisances qu'ils nous ont fournit lors de notre formation, sans quoi ce projet n'aurait pas eu lieu.

Table des matières

1 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 à 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 déroulé du 17 octobre 2014 au 1er mai 2015. Durant cette période, nous avons été formé à la gestion de projet par M. Rémi DIONISI ainsi que M. Karim ABDELLAH GODARD.

Le thème de ce projet tourne autour d'OpenPGP. Le sujet se décompose en trois parties. La première partie consistait en la rédaction d'une étude d'OpenPGP et de son implantation en ligne de commande GnuPG. La deuxième partie a été l'implantation d'une interface graphique pour GnuPG. Enfin la troisième fut l'implantation et l'explication d'une attaque sur OpenPGP.

Dans un premier temps, il nous semble nécessaire de vous parler plus en détail du contexte de ce projet. Nous vous présenterons ensuite ce qui a été réalisé, puis nous ferons état des problèmes rencontrées. Enfin, pour finir nous effecturons un bilan de ce projet.

2 Contexte

2.1 OpenPGP

OpenPGP est un un standard normalisé dans la RFC 4880 qui définit des format de messages. Ces formats reposent sur de la cryptographie hybride, c'est à dire une combinaison de clefs symétriques et asymétriques. Ils permettent de fournir des services de sécurité pour les communications électorniques ainsi que le stockage de données. Ces services quand à eux, oeuvrent pour garantir :

- la confidentialité (seuls les destinataires du messages peuvent le déchiffrer),
- l'authenticité (l'émetteur d'un message est bien celui qu'il prétend être),
- l'intégrité (l'état des données transmisent est le même qu'au moment de l'envoi, elles n'ont pas été altérées).

2.2 GnuPG

GnuPG est une implémentation libre du standard OpenPGP. Ce logiciel a pour but de proposer une alternative au logiciel PGP qui lui, est une implémentation non libre. GnuPG permet de signer, vérifier (assure l'authenticité et l'intégrité), chiffrer et déchiffrer (assure la confidentialité) des fichiers, ainsi que de gérer un trousseau de clefs cryptographiques (asymétriques) permettant ces actions. Un modèle de toile de confiance est associé au trousseau de clefs. Ce modèle permet de gérer pour chaque clefs du trousseau une validité pour garantir qu'elle appartient bien à la personne identifié, ainsi qu'un niveau de confiance en cette personne.

2.3 Le besoin

Il existe quelques interfaces graphiques (comme KGpg, GPA, Seahorse). Cependant, ces interfaces ne permettent pas une gestion fine des clefs et la partie toile de confiance n'est pas correctement représentée. Il nous a donc été demandé de proposer une interface graphique permettant à un utilisateur novice en PGP, mais averti en sécurité, de faire facilement des réglages techniques sur son trousseau et de pouvoir mettre en place sa toile de confiance. Le logiciel doit donc être à la fois pédagogique, précis et accompagné d'un document d'explications et de recommandations d'utilisation. Il doit aussi fonctionner sous kde et gnome.

Nous devions aussi réaliser une étude complète d'OpenPGP et du logiciel GnuPG (en ligne de commande), d'en comprendre le fonctionnement détaillé et de rédiger un rapport illustrant toutes les fonctionnalités.

Enfin, nous devions effectuer des recherches sur les limites cryptographiques de PGP et produire un

document d'analyse de ces limites. En particulier il était demander d'implanter l'attaque sur les identifiants de clefs PGP décrite dans le numéro 75 de MISC magazine.

2.4 Acteurs du projet

La cliente de ce projet est Mme. Magali BARDET (enseignante et responsable du master SSI à l'UFR des sciences et techniques de Rouen).

M. Karim Abdellah GODARD est un intervenant extérieur et a assuré le rôle de formateur et consultant en gestion de projet.

L'équipe en charge du développement était constituée de sept étudiants actuellement en première année du master SSI de Rouen :

- Bertille BOUILLIE — Reponsable client
- Guillaume LEROY — Architecte
- Ibrahima Sory BARRY — Chargé client
- Lucas BARBAY — Testeur
- Matthieu FIN — Responsable technique
- Pierre BALMELLE — Responsable qualité
- Olivier THIBAULT — Chef de projet

2.5 L'organisation

Ce projet a été réalisé dans le cadre de la première année du Master Sécurité des Système 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.

3 Présentation du projet

3.1 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.

3.2 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.

4 Les problèmes rencontrés

Lors de la réalisation de ce projet nous avons du faire face a différents problèmes aussi bien d'ordre organisationnel que techniques, auxquels nous avons du remédier.

4.1 Problèmes organisationnel

Les difficultés organisationnelles rencontrées sont essentiellement survenues du fait de la modification de l'effectif de l'équipe durant la phase de réalisation du projet.

L'équipe initialement formée de sept développeurs, s'est trouvé réduite de deux personnes :

— Bertille Bouillie qui dès les deux premières semaines n'a plus donné aucune nouvelle, son abandon a seulement pu être officiellement pris en compte au bout d'un mois et demi.

— Guillaume Leroy qui a abandonné le projet au bout d'un mois et demi.

De plus les actions entreprises lors de l'avant projet n'ont pas suffi à l'ensemble de l'équipe pour se former sur les différents outils utilisés lors de la phase de réalisation, puisque lors du premier sprint toutes les tâches attribuées a certains membres n'ont pas pu être réalisées suite a ces différentes lacunes.

Nous avons, suite à cela pris du retard sur le premier sprint.

Un plan d'action a alors été mis en place pour faire l'état des lieux des tâches faites, et des tâches réalisables avec le restant de l'équipe et le temps disponible.

Ce plan a été présenté et discuté avec le client pour redéfinir le périmètre du projet.

Suite à cela nous avons du réattribuer les tâches a chacun pour pouvoir tenir la charge de travail, Lucas et Ibrahima ont souhaité se charger respectivement de l'attaque et de l'étude d'OpenPGP / GPG.

Ainsi nous avons redéfini les tâches de développement de l'application entre Olivier, Matthieu (développeurs) et Pierre (Testeur). Les fonctionnalités de l'application on également été redéfinies pour pouvoir être réalisable avec un effectif aussi réduit.

De plus toute la réalisation de la visualisation de la toile de confiance a été réduite à l'affichage des niveaux de confiance d'une clé et non plus en dessin d'une toile de confiance graphique.

Nous avons également a la fin du premier sprint suite à ces observations redéfinir les rôles de chaque membres :

Noms	**Rôles**
Olivier Thibault	Chef de projet / Développeur
Matthieu Fin	Architecte / Chargé client / Développeur
Pierre Balmelle	Testeur
Lucas Barbay	Chargé de l'attaque
Ibrahima Sorry Barry	Responsable de documentation OpenPGP / GnuPG

4.2 Problèmes techniques

4.2.1 Maîtrise des outils

Lors de la phase d'avant projet nous avons organisé des sessions d'entraînement afin de prévenir du risque lié a l'incompréhension des outils utilisés tels que git, Qt, le langage C++, ou même le logiciel GnuPG.

Seulement même si lors de l'avant projet l'ensemble de l'équipe semblait maîtriser ces différents outils nous nous sommes rendu compte lors de la phase de développement que ce n'était pas le cas pour tout le monde.

Les outils utilisés ont été définis conjointement dès le 27 novembre, or dès le début de la phase de développement (c'est à dire au mois de janvier) certain membres n'avaient toujours pas installé les dits outils. Par conséquent ils ne pouvaient les maîtriser. Nous avons donc dû nous réunir pour installer et former a minima les différents membres sur ces outils, ce qui nous a fait perdre du temps sur le premier sprint de développement.

4.2.2 Maîtrise de GnuPG

4.2.3 Communication GnuPG

5 Bilan du projet

5.1 Compétences acquises

5.1.1 Technique

5.1.2 Organisationnel

5.2 Axes d'amélioration

5.3 Rétrospective

6 Conclusion