

Soutenance projet annuel - Chat sécurisé

Charles Ango - Ismaël Kabore - Julien Legras - Yves Nouafo -
Jean-Baptiste Souchal

Master 1 Sécurité des Systèmes Informatiques

31/05/2013



Sommaire

- 1 Présentation du projet
- 2 Déroulement des sprints
 - Sprint 1
 - Sprint 2
 - Sprint 3
- 3 Technique
- 4 Certificats
- 5 Module sécurisé
- 6 Difficultés rencontrées
- 7 Conclusion

Présentation du projet

Sujet proposé par Magali Bardet

Réaliser un logiciel de messagerie instantanée **sécurisée** : client et serveur.

S'inspirer des fonctionnalités d'IRC (Internet Relay Chat).

Fonctionnalités demandées :

- gestion de la création et la suppression d'un compte sécurisé ;
- création par un utilisateur d'une salle de discussion pour un groupe de personnes ;
- ajout/suppression d'un utilisateur autorisé dans une salle ;
- assurance de confidentialité, d'intégrité et d'authentification sur les messages échangés ;
- non-répudiation des messages.

Sprint 1

Livraison

Tests : OK

Délai respecté (15 février 2013)

Réunion avec Mme Bardet post livraison le 19 février pour validation

Tâches

Retard cumulé : 1 jour

Raison(s) : prise en main de SQLite

Sprint 2

Livraison

Tests : OK

Délai respecté (15 mars 2013) : livraison d'une machine virtuelle
↪ mise à disposition d'une machine par Mr Macadré (configurée lors du sprint 3)

Réunion avec Mme Bardet post livraison le 3 avril pour validation

Sprint 3

Livraison

Tests : OK

Délai réajusté avec Mme Bardet (3 mai 2013)

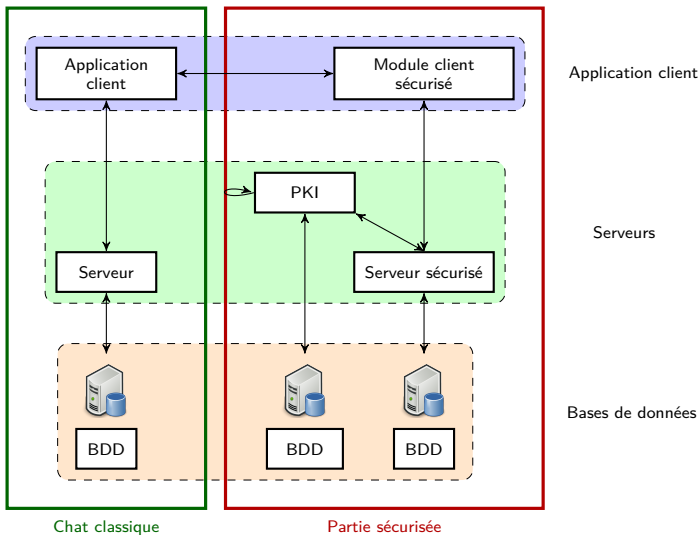
Réunions avec Mme Bardet pré livraison le 29 avril et post livraison le 22 mai

Tâches

Retard : 3 semaines

Raison(s) : contrôles continus pendant 2 semaines + 1 semaine *off*

Schéma global



Certificats

Génération de requête

```
$ openssl genrsa -out maclef.pem 2048
```

```
$ openssl req -new -key maclef.pem -out marequete.req
```

Récupération du certificat

- 1 Faire une demande à l'administrateur de la PKI
(julien.legras@etu.univ-rouen.fr)
- 2 Se rendre sur :
`http://inf-srv-securechat:
8080/ejbca/enrol/server.jsp`

Module sécurisé

Authentification

Clef RSA 2048 bits certifiée par notre PKI

↔ tunnel SSL entre serveur sécurisé et client sécurisé (double authentification)

↔ vérification chaîne de certification

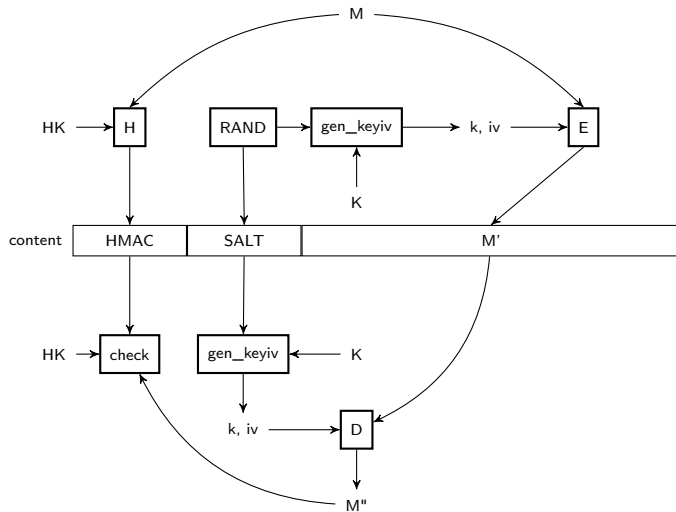
Chiffrement des messages

AES-256-CBC (Cipher Block Chaining)

Master key générée et transmise aux destinataires lors de :

- création de salon
- ajout/retrait/déconnexion d'utilisateur d'un salon

Clef/IV générées à partir de la master key et d'un sel pseudo-aléatoires (EVP_BytesToKey + RAND)



Difficultés rencontrées

Gestion de projet

- format livraison PKI
- surcharge de travail
- difficulté d'intégration des tests de sécurité dans le cahier de recettes

Techniques

- apprentissage OpenSSL
- GTK et threads

Conclusion I

Bilan

- Utilisation des documents de projets → meilleure planification du développement et actions systématiques
- Communication, confrontation d'idées dans l'équipe de développement grâce à la méthode agile scrum
- Apprentissage techniques en sécurité : certification (EJBCA), OpenSSL (bibliothèque et commandes)
- Interface graphique du C grâce au Vala

Conclusion II

Améliorations envisageables

- Gestion de plusieurs serveurs par le client
- Renouvellement régulier des clefs de chiffrement symétrique
- Internationalisation de l'application (POT)
- Portage multi-plateformes (couche réseau)
- Amélioration client lignes de commandes (NCurses)