Plan de développement

Version	1.0
Date	11/12/2013
Rédigé par	Pascal Edouard
Relu par	X
Approuvé par	X

MISES À JOUR

Version	Date	Modifications réalisées
1.0	14/12/2013	Création du document

Table des matières

1 Objet

Le projet s'inscrit dans un cadre relatif aux faits d'actualités autour de la sécurité, notamment concernant la crédibilité des fonctions de génération de nombre aléatoire ou encore sur l'application des standards dans les fonctions d'OpenSSL.

RSA et DSA peuvent échouer lamentablement lorsqu'ils sont utilisés par un mauvais générateur de nombre aléatoire mais combien de cas comme celui ci peut-il y avoir sur le web ? La première partie de ce projet essaiera de répondre à cette question en faisant un état des lieux des serveurs TLS et SSH et présenter des évidences que des clefs vulnérables peuvent exister.

La deuxème partie de ce projet consistera à étudier les fonctions d'openSSL, en particulier sa partie développant la génération d'éléments aléatoires et ses primitives cryptographiques. Chaque fonctions seront comparer avec les standards actuels (cf. PKCS) afin de déterminer si elle est efficace.

Enfin, la troisième partie de ce projet consiste à développer une application tournant sur serveur sécurisé afin d'analyser chaque machine cliente se conectant à celui ci. L'application possèdera une liste de critères et des menaces éxistantes, par exemple avec la validité du certificat du client présenté lors de la connexion, afin de tester la machine cliente et en déduire si elle est potentiellement un risque pour le serveur.

Ce projet est réalisé dans le cadre de l'enseignement de premère année de master Sécurité des Systèmes Informatiques. Il sera réalisé par un groupe de cinq étudiants. La première partie du projet consiste à rédiger les documents qui nous permet de mieux définir le sujet, les objectifs, les risques et l'organisation du projet. Suite à cela, le développement des différentes applications commenceront sur une durée de 6 semaines.

Documents de référence :

- Mining Your Ps and Qs : Detection of Widespread Weak Keys in Network Devices
  by Nadia Heninger, Zakir Durumeric, Eric Wustrow, J. Alex Halderman
- ZMAP

2 Terminologie et sigles utilisés

- **RSA/DSA :** Advanced Encryption Standard et Digital Signature Algorithm, sont deux algorithmes de chiffrement à bi-clef (publique et
  privée)
- **Appli RC :** Application de Récupération des certificats
- **Appli F :** Application de Factorisation
- **Certificat :** Document élétronique utilisant une signature digitale afin de liéer une clef plublique à une identité

3 Méthodologie de développement

Ce projet reposera sur la méthode agile en prenant en compte ses valeurs culturel et principes en l'appliquant dans une méthodologie SCRUM afin d'apporter une discipline de développement et de délivrer les résultats dans les meilleurs conditions.

Ce qui captive l'utilisation de la méthode Agile est l'essence et la philosophie de son approche et les points valoriser telle que :

- Les individus et leurs interactions plus que les processus et les outils :

Elle correspond à la communication entre les collaborateurs à tout les niveaux (client/fournisseurs, testeurs/programmeurs afin de ne pas perdre de temps ni d'énergie dans les malentendus ou incompréhension.

- La collaboration avec les clients plus que la négociation contractuelle :

Une approche direct avec le client qui se sent beaucoup plus impliqué dans le projet afin de le permetre d'apporter ses avis et remarques.

- L'adaptation au changement plus que le suivi d'un plan :

Être capable de s'adapter lorsqu'une modification importante est nécessaire.

Ainsi, une grande priorité sera de satisfaire les demandes du client en livrant régulièrement des fonctionnalités, tester préalablement par des outils de tests développés, et les faire valider par le client. Chaque fonctionnalité implementée sera intégrée au projets et testée.

La méthodologie de Scrum représente correctement cette approche dans le cadre de notre projet. Il est rythmé par un ensemble de réunions clairement définies et stritement limitées dans le temps :

- **Planification du Sprint** (Sprint = itération) : au cours de cette réunion, l'équipe de développement sélectionne les éléments prioritaires du « Product Backlog » (liste ordonnancée des exigences fonctionnelles et non fonctionnelles du projet) qu'elle pense pouvoir réaliser au cours du sprint (en accord avec le « Product Owner »).
- **Revue de Sprint** : au cours de cette réunion qui a lieu à la fin du sprint, l'équipe de développement présente les fonctionnalités terminées au cours du sprint et recueille les feedbacks du Product Owner et des utilisateurs finaux. C'est également le moment d'anticiper le périmètre des prochains sprints et d'ajuster au besoin la planification de release (nombre de sprints restants).
- **Rétrospective de Sprint** : la rétrospective qui a généralement lieu après la revue de sprint est l'occasion de s'améliorer (productivité, qualité, efficacité, conditions de travail, etc) à la lueur du « vécu » sur le sprint écoulé (principe d'amélioration continue).
- **Mêlée quotidienne** : il s'agit d'une réunion de synchronisation de l'équipe de développement qui se fait debout (elle est aussi appelée « stand up meeting ») en 15 minutes maximum au cours de laquelle chacun répond principalement à 3 questions : « Qu'est ce que j'ai terminé depuis la dernière mêlée ? Qu'est ce que j'aurai terminé d'ici la prochaine mêlée ? Quels obstacles me retardent ? »

4 Organisation et responsabilités :

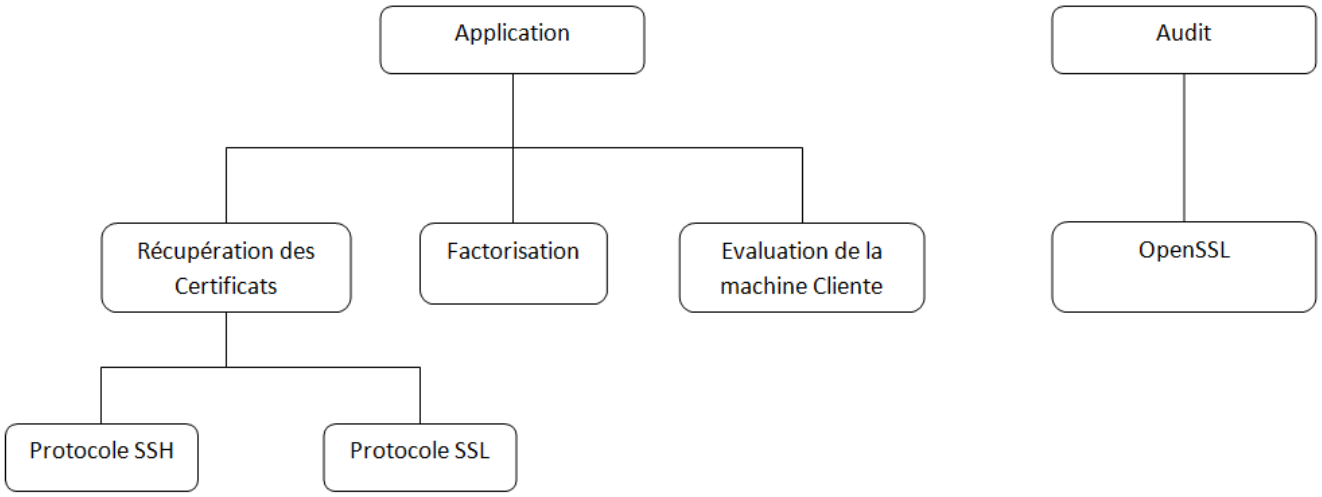
Lors de la première et la troisième partie du projet, qui consiste au développement de différente application, chaque membre de l'équipe sera assigner un rôle particulier :

Développeur
: responsabes de la production du code. Ils aident aussi à la ré-estimation de la charge de travail en fonction de l'avancement du projet. Ces rôles sont tenus par Julien LEGRAS et Pascal EDOUARD.

Client
: notamment le «Product Owner», qui porte vision du produit à réaliser et représente généralement le client afin d'assurer l'intermédiaire avec l'équipe. Ce rôe est tenu par Claire SMETS.

Coach
: notamment le «Srum Master», reste le garant de l'application de la méthodologie Scrum et de l'équipe en terme de communication et le fonctionnement. Ce rôle est tenu par Pascal EDOUARD.

5 Organigramme des tâches :



6 Evaluation du projet :

L'approche Scrum commence par lister les exigences du client afin de produire le « Product Backlog ». On définit une unité de coût (en terme de complexité) avec la colonne Estimation. Elle permet de faciliter l'ordonnacement du Product Backlog, la planification des sprints et des releases.

7 Dimensionnement des moyens :

Nous avons besoin, pour ce projet, d'une bonne connexion avec internet afin de récupérer le maximun de certificats avec le mininum de perte de connexion possible. Une machine moyenne (normal) en terme de performance est nécessaire pour cette partie. Cependant, l'application de factorisation des moduli nécéssite quelque chose de beaucoup plus puissante en terme de disque, mémoire et calcule de processeur. Nos possibilité d'obtenir un serveur de cette taille varie de possibilité, du plus probable au moins évident :

1. Serveur local de l'université,
2. Serveur de calcul au CRIHAN,
3. Serveur Amazone à un prix raisonable.

Le code source ainsi que les différents documents produits sont stockés sur le serveur GIT : (https ://github.com/randomguys)

8 Description des tâches :

		Tâche	Description	Dépendances
Sprint 1	**App. RC**	1	Récupération de la liste des adresses IP des serveurs	
		2	Récupération des certificats SSH	1, 6
		3	Stockage des certificats SSH	1,6
		4	Récupération des certificats SSL/TLS	2
		5	Stockage des certificats SSL/TLS	1, 6
	App. F	1	Extraction des clefs des certificats	
		2	Trouver des facteurs communs des clefs récupérées	2
Sprint 2	**OpenSSL**	1	Lister les fonctions d'OpenSSL à auditer	1, 6
		2	Lister les standards utilisé par chaque fonctions à auditer	3, 8
		3	Auditer les fonctions d'OpenSSL listées	
		4	Mettre en place la page web des résultats de l'audit	10.1
Sprint 3	**App. Eva**	1	Lister les critères à vérifier sur une machine cliente	
		2	Dévelopement d'une fonction pour chaque critère	1.1, 4
		3	Récupération des données du navigateur	1.1, 3
		4	Evaluer chaque critère de la machine Cliente	
		5	Ajouter une page web pour les résultats de l'évaluation	2

9 Gestion de la documentation :

Les documents de référence pour la gestion de ce projet seront disponible au format pdf sur le serveur de GIT.

Chaque membre est responsable d'un document livrable, qui évolue au fil du projet et sera incrémenter par un numéro de version :

- Le Spécification Technique du Besoin : Claire SMETS
- Le Document d'Architecture Logicielle : Julien LEGRAS
- L'Analyse des Risques : Pascal Edouard
- Le Cahier des Recettes : Mathieu LATIMIER et William BOISSELEAU
- Le Plan de Développement : Pascal EDOUARD

L'ensemble du groupe devra se tenir au courant de l'évolution de chaque document. De plus, après chaque réunion avec le client, un compte rendu sera rédigé et validé par l'équipe avant d'être soumis au client, qui pourra ensuite le valider. Le compte rendu sera accéssible sur le serveur de document GIT.