HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Travail de Bachelor 2020

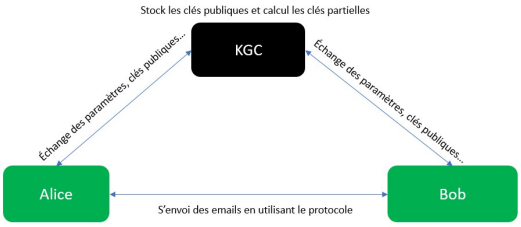
Chiffrement / signature d'emails

Introduction

Ce travail de Bachelor consiste à mettre en application une primitive cryptographique pouvant donner plus de possibilités que PGP ou S/MIME et plus facile à mettre en place. En effet, ces protocoles souffrent de problèmes de conception. C'est ainsi que des failles telles que EFAIL ont vu le jour, permettant de récupérer le texte clair d'un mail chiffré à l'aide de PGP ou S/MIME. Pour cela une analyse a été faite sur différents systèmes de mails sécurisés incorporant une variété de façon de chiffrer des emails (très souvent à l'aide de PGP).

Architecture

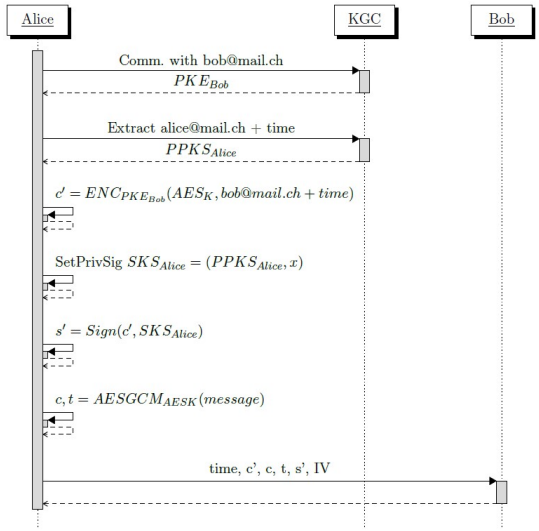
C'est ainsi que ce travail s'oriente vers une primitive peu connue qu'est le Certificateless Public Key Cryptography. Cette primitive se basant sur l'Identity Based Encryption permet de lier une identité (ici l'email de l'utilisateur) à sa clé publique, ceci sans avoir à mettre en place une PKI (Public Key Infrastructure) et des certificats difficiles à gérer dans un système global de mail. Voici l'architecture nécessaire entre deux utilisateurs qui veulent s'envoyer un mail :



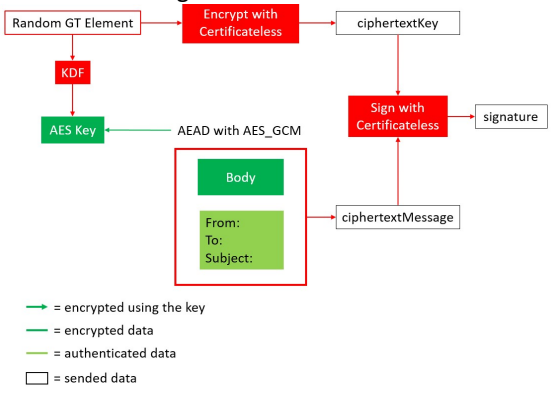
Une fois l'étude de cette primitive faite, une modification a été apportée pour avoir une propriété cryptographique en plus. La Forward Secrecy, propriétés non fournies par S/MIME ou PGP permettant au système de ne pas dévoiler tous les textes clairs si une fuite de clé privée venait à arriver.

Exemples

Un Proof Of Concept a été fait utilisant cette primitive pour chiffrer / déchiffrer et signer / vérifier un mail. Voici le cas de l'envoi d'un mail :



Comme on peut le voir sur le schéma ci-dessus, le protocole créé implémentes un système hybride de chiffrement utilisant la cryptographie asymétrique et symétrique. Dans la figure suivante l'on peut apprécier une vue globale du système de chiffrement et signature d'email.



Auteur: **Mickael Bonjour**
Répondant externe:
Prof. responsable: **Alexandre Duc**
Sujet proposé par: **Alexandre Duc**

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale