Chiffrement Unidirectionnel et Chiffrement Bidirectionnel

Constructions, Modèle de Sécurité et Applications

Mamadou Makhtar LO

January 7, 2021

Introduction

Contexte

- Développements Technologiques: Cloud Storage, Cloud Computing, IoT etc..
- Partage de fichiers entre utilisateurs
- Besoins en Sécurité: Délégation, Contrôle d'accès..
  Comment partager un fichier sans divulguer le message ou les clé de déchiffrements ?

Introduction

Objet:

Serveur de re-chiffrement (ou Proxy Re-Encryption)

- Transforme un texte chiffré pour une clé particulière en un texte chiffré pour une autre clé:
  sans avoir accès au texte clair,
  sans avoir accès aux clés de déchiffrement.
- Selon le sens de la délégation: Chiffrement Unidirectionnel Chiffrement Bidirectionnel.

Introduction

Problématique

- Construction de serveurs de re-chiffrement (unidirectionnel/Bidirectionnel)
- Preuves de Sécurité
- Applicabilité et efficacité

Introduction

Objectifs

- Aspects définitionnels de la notion de PRE (définitions, particularités, modèles existants ...)
- Aspects cryptographiques théoriques (Proposition de modèles, analyse de la sécurité, applications...)
- Aspects cryptographiques pratiques (Implémentation, tests d'applicabilité...)

Serveur de re-chiffrement (PRE)

Proxy Re-Encryption

- Proposé en 1998 par Matt Blaze, Gerrit Bleumer et Martin Strauss
- "Atomic Proxy function"
- Développement (Méthode générique 2003, Formalisation en 2005 etc..)

Principe de fonctionnement

PRE: $\{$*Clé*, *Délégation*, *Chiffrer*, *Re-Chiffrer*, *Dechiffrer*$\}$ tels que:

- *Clé* génère les clés de chiffrement et déchiffrement.
- *Délégation* génère la clé de délégation ou *clé proxy*.
- *Chiffrer* chiffre le message à l'aide de la clé de chiffrement.
- *Re-Chiffrer* transforme (re-chiffre) à l'aide de la *clé proxy* un texte chiffré pour A en un texte chiffré pour B.
- *Dechiffrer* déchiffre le texte chiffré à l'aide de la clé de déchiffrement.

Chiffrement Unidirectionnel

Chiffrement Bidirectionnel

Le schéma "lite" Cramer-Shoup

Le schéma "lite" Cramer-Shoup

Chiffrement Bidirectionnel

Conclusion