Rapport Sécurité des systèmes autonomes

Synthèse d'un article de recherche sur
« le chiffrement à préservation de format »

Rapport rédigé par : Yasmina AIT ALI

Le 26 /12/2017

A. Terence Spies,Chiffrement à préservation de format,Voltage Security, Inc.

1. Introduction

Chiffrer les informations personnelles identifiables (PII) , dans les grandes bases de données a toujours été difficile, et l'un des obstacles à l'adoption des méthodes de chiffrement efficaces est le coût de la modification des bases de données , et des applications à accueillir des informations cryptées.Ces coûts sont généralement associés à deux changements nécessaires pour prendre en charge les données classiquement cryptées comme les numéros de carte de crédit ou les numéros de sécurité sociale , qui sont souvent utilisés comme des clés ou des indices dans les bases de données, donc la randomisation de ces champs en cryptant des données peut nécessiter un changements significatifs du schéma.Deuxièmement, les applications peuvent être écrites en attendant des données dans un format spécifique ,du moment que le cryptage étend généralement les données et nécessite un changement de format.Par exemple le numéro de carte de crédit est une série de 16 chiffres,si on les chiffre avec AES,on obtient une chaîne plus longue qui peut contenir jusqu'à 54 bits et qui ne correspond plus au format initial de la chaîne des 16 chiffres entiers en claire .

La réponse à se problème s'appelle "Format-Preserving Encryption", ou FPE. Comme son nom l'indique, l'objectif d'un schéma de cryptage de conservation de format est de crypter de manière sécurisée tout en préservant le formatage original des données en texte brut.Cela signifie, en un mot, que notre numéro de carte à 16 chiffres peut être crypté en un nombre de16 chiffres.

2. Modèle FPE:

Pour une utilisation sécurisée de FPE sur une base de données interne,tout mécanisme de sécurité doit être fort avec les limitations suivantes:

Contrainte 1:L'attaquant connaît le format et le type de données dans la base de données.Nous devrions supposer qu'un attaquant sait qu'il cherche ,numéros de carte de crédit ou numéros de sécurité sociale.

Contrainte 2: La taille du texte en clair sera relativement petite, par rapport à la taille d'ensembles cryptographiques.Cela signifie que tout mécanisme FPE doit protéger contre l'accès de l'attaquant à la fonction crypter / décryptes.

Contrainte 3: Les données ne peuvent pas être étendues.Lorsqu'un algorithme FPE crypte un numéro à N chiffres, il doit émettre un nombre à N chiffres.

Contrainte 4: Les données doivent être cryptées de manière déterministe.

Les données sont généralement étant crypté dans une base de données, et il est hautement souhaitable pour préserver la possibilité d'utiliser une colonne comme une clé ou un index.

3. Méthodes FPE:

On spécifie trois méthodes de cryptage de conservation de format(FPE), appelées la méthode Préfixe, Cycle-walking et Feistel-Cycle. toutes dérivées dans le document Black et Rogaway, et Chacune de ces méthodes est un mode opératoire de l'algorithme AES, qui est utilisé pour construire une fonction circulaire dans la structure de Feistel pour le chiffrement.en notant que chacune des trois méthodes gère une taille d'ensemble d'entrée différente, soit pour la sécurité ou pour la performance.

3 .1 La méthode Préfixe, est très simple, en revanche elle fonctionne que sur de petits ensembles de données.La méthode fonctionne en écrivant une permutation aléatoire en mémoire, et en utilisant cette permutation pour crypter des données.

La méthode de préfixe peut être considérée comme ayant un temps de configuration de clé très lent (la permutation en mémoire) et un temps de cryptage et de décryptage très rapide.

3.2 La méthode du Cycle-walking : comme la méthode Préfixe, sa construction est assez simple, mais elle fonctionne sur une série limitée d'ensembles. Le cycle-walking fonctionne en cryptant le texte en clair avec un chiffrement de bloc existant (AES ou 3DES) à plusieurs reprises jusqu'à ce que la sortie du chiffrement tombe dans la plage de sortie acceptable.Ceci dit N doit être un petit nombre de bits plus courts que la sortie du chiffre,pour que cette opération se termine en un temps raisonnable.

Pour la sécurité de cette méthode,elle a été prouvée que sa construction ne dégrade jamais la sécurité du chiffrement sous-jacent.

3.3 Feistel + méthode de cycle : c'est la méthode la plus complexe que la construction Préfixe ou Cycle-walking, mais elle permet un cryptage sur une grande variété de tailles d'ensembles ,elle fait passer un texte de n bits en clair par plusieurs tours en utilisant une fonction pseudo-aléatoire (PRF) f, qui prend n / 2 bits et renvoie n / 2 bits, divisé en deux moitie ,partie gauche et droite, appelée L et R,ainsi la fonction ronde produit un nouveau L et R, en sortie ou bien renvoyée dans le tour suivant.

R '= L XOR f (R)

L '= R

La sécurité de ce chiffre peut être mesurer de trois manières différentes.attaquer par le meilleur attaquant possible,la deuxième est la résistance à l'attaque par la force brute et la troisième est le meilleur attaquant connu qui est l'attaque la plus connue qui distingue les réseaux Feistel de permutations aléatoires.Et généralement,pour répondre à toutes les limites de sécurité l'algorithme de Feistel est appliqué à de 8 jusqu'à 16 tours.

4. Exemple applicatif du format de préservation de chiffrement:

Cas de numéros de carte de crédit

L'application du chiffrement à préservation de format sur le numéros des cartes de crédit s'avère très intéressant ,car le numéro de la carte de crédit porte un chiffre de contrôle à la fin du nombre qui est calculé avec le Algorithme de Luhn, qui est une somme modifiée des chiffres , et qui n'a pas besoin d'être chiffré. Il existe trois méthodes de chiffrement avec cette somme de contrôle:

Méthode 1 - chiffrement transparent :

Pour ce faire, chiffrer tous les chiffres, sauf le dernier en utilisant un algorithme de FPE. Après le cryptage, ajouter un chiffre de contrôle avec une somme de contrôle valide des chiffres chiffrés. Pour décrypter, FPE déchiffrer tous les chiffres à l'exception du dernier,puis régénérer les chiffres de somme de contrôle sur le chiffres en texte brut.

Méthode 2 - Marquage Checksum :

Chiffrer le nombre mais en excluant le dernier chiffre, et remplacer le chiffre de contrôle avec la valeur de contrôle plus 1. Ceci assure que le chiffre de contrôle est invalide, et donne un méthode fiable pour distinguer un CCN crypté d'un CCN en clair.

Méthode 3 - codage de Checksum :

Cette méthode consiste à faire un décalage de la somme de contrôle,qui peut être utilisé pour coder un petit ensemble d'informations supplémentaires dans le chiffre de la somme de contrôle. Cela peut être utilisé pour sélectionner parmi un ensemble de clés, en ajoutant la diversité à un existant schéma de gestion des clés. Générer neuf clés, crypter tous les chiffres avec une de ces clés, et remplacer les chiffres de la somme

de contrôle avec la somme de contrôle plus une valeur d'identification de clé de 1 à 9. Ce qui assure que le checksum est invalide, et donne une méthode pour changer les clés et enregistrer quelle clé est utilisée pour crypter l'information.

5. Conclusion:

En effet l'article décris la méthode de chiffrement à préservation de format, et son efficacité dans le chiffrement des informations personnelles identifiables (PII) . Ainsi l'auteur de cet article nous a bien présenté un cas pratique très intéressant et courant ,qui est l'application de cette méthode FPE sur les numéros de cartes de crédit, qui s’avère répondre à la problématique posée dans ce rapport et elle respecte toutes les limites de sécurité exigées.