Pascal.Junod@epfl.ch, en cours de thèse au Laboratoire de Sécurité et de cryptographie

Six façons différentes de casser DES

Introduction

DES (Data Encryption Standard) est un algorithme de chiffrement à clé secrète qui a été adopté comme standard pour une utilisation non-militaire aux Etats-Unis en janvier 1977 par le *National Bureau of Standards* [1]. Il est extrêmement répandu dans bien des domaines d'applications, qui vont du simple chiffrement d'un document à l'authentification de transactions bancaires électroniques.

Dans cet article, nous nous proposons de présenter six façons différentes de *casser* DES qui ont été découvertes aux cours de ces dernières années.

Recherche exhaustive

DES est un algorithme capable de chiffrer un bloc de données P de 64 bits à l'aide d'une clé secrète K de 56 bits. Le résultat est un bloc de données chiffrées de 64 bits que nous noterons C. L'opération de déchiffrement $P=D_K(C)$ est, grâce à la structure même de l'algorithme, quasiment identique à l'opération de chiffrement $C = E_K(P)$, la seule différence étant une légère modification de la préparation de la clé.

Imaginons que nous disposions d'un bloc de données chiffrées *C'* et que nous voulions trouver la clé secrète correspondante. Si nous disposons d'un peu d'information sur la structure ou le contenu des données en clair (texte ASCII, image JPEG, paquet de réseau ayant une structure connue,…), la méthode la plus simple est une recherche exhaustive de la clé correspondante parmi les $2^{56} \sim 7.2 \bullet 10^{16}$ possibilités. Le principe, très simple, est le suivant: une clé après l'autre, on essaye de déchiffrer le bloc de données, l'information sur le texte clair nous permettant de reconnaître la bonne et donc d'interrompre la recherche. Nous aurons besoin, en moyenne, de 2^{55} essais avant de terminer notre attaque.

Une machine dédiée

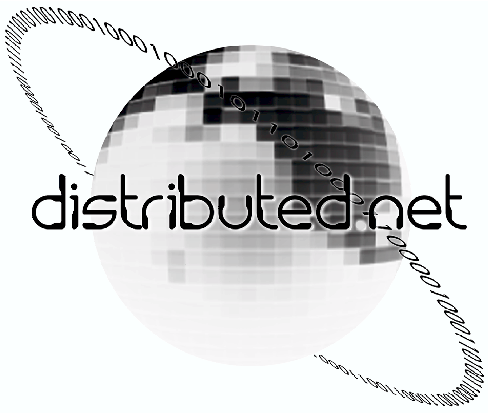
La complexité, mesurée en terme de quantité de calcul, d'une recherche exhaustive est certes énorme, mais à présent, grâce aux progrès de la technologie des microprocesseurs depuis 1977, elle est loin d'être inaccessible. DES est un algorithme orienté hardware qui a le gros désavantage pour le cryptanalyste d'être très lent en software. Une plate-forme PC actuelle, à savoir un processeur Intel Pentium III 666MHz, peut examiner environ 2 millions de clés par seconde, ce qui implique un temps de recherche moyen de 600 années pour un seul PC.

Une solution matérielle a été proposée et réalisée par l'EFF (Electronic Frontier Fundation) en 1998, dans le seul but de prouver que DES n'est pas (ou plus) du tout un algorithme sûr. **Deep Crack** [2], tel est le nom de cette machine extraordinaire, a coûté moins de 210'000 $. Elle est constituée de 1536 chips qui sont capables de décrypter un bloc en 16 cycles d'horloge, le tout étant cadencé à 40 MHz. Ces caractéristiques lui donnent la possibilité d'examiner 92 milliards de clés par seconde, ce qui donne un temps de recherche moyen situé entre 4 et 5 jours.

Vu le budget modeste de l'EFF, il n'est pas difficile de tirer des conclusions alarmistes sur la sécurité de DES vis-à-vis d'organismes gouvernementaux (tel la NSA, organe américain chargé de l'espionnage électronique [7]) ou d'organisations criminelles.

Un gigantesque cluster

Il n'est même pas nécessaire de disposer de gros moyens financiers pour pouvoir casser DES. De la bonne volonté et quelques bénévoles sont suffisants. Le 19 janvier 1999, dans le cadre d'un concours sponsorisé par une des entreprises majeures en sécurité informatique, RSA Labs, a cassé une clé en moins de 23 heures. L'organisation **distributed .net** [3] regroupe des milliers d'ordinateurs (de la machine la plus simple aux serveurs multiprocesseurs les plus puissants) sur Internet qui fournissent gracieusement leur puissance de calcul à disposition lorsqu'ils sont inactifs. Plus de 100'000 ordinateurs ont reçu un certain nombre de clés à contrôler via le réseau, ce qui a permis un taux de traitement de 250 milliards de clés par seconde.



Un compromis temps-mémoire

Nous avons déjà abordé l'idée de recherche exhaustive de clé: on a à disposition un couple texte clair - texte chiffré et on essaye les 2^{56} clés possibles. Cette méthode ne demande quasiment aucune mémoire, mais en contrepartie, on devra essayer en moyenne

2^{55} clés avant de tomber sur la bonne. D'un autre côté, il serait imaginable, pour un texte clair x donné, de précalculer le texte chiffré $y = E_K(x)$ correspondant pour toutes les 2^{56} clés K, et de stocker les paires (y_K, K) triées par leur première coordonnée.

Plus tard, lorsque l'on obtient un texte chiffré y à partir de x, il est possible, par une simple recherche dans notre table, de retrouver la clé correspondante. Nous pouvons noter que cette recherche demande un temps constant; par contre, nous avons un besoin énorme de mémoire (1.5 milliard de Go), ainsi que de beaucoup de temps pour construire cette table. De plus, le bénéfice ne devient effectif que si l'on doit chercher plus d'une clé à partir du texte chiffré d'un même message.

Un algorithme, dit de *compromis temps-mémoire*, a été proposé en 1980 par Hellman [4]. Il combine à la fois une demande de mémoire moindre que celle de notre proposition, ainsi qu'un temps de calcul inférieur à celui d'une recherche exhaustive. Cette attaque demande environ 1000 Go de capacité de stockage et 5 jours de calculs sur un simple PC.

Cryptanalyse différentielle

En 1990, deux chercheurs israéliens du Weitzmann Institute, Biham et Shamir, ont présenté une nouvelle attaque, la cryptanalyse différentielle [5]. En utilisant cette méthode, les deux chercheurs ont proposé pour la première fois une façon de casser DES qui demande moins de temps de travail qu'une recherche exhaustive.

Imaginons que nous disposions d'un boîtier électronique capable de chiffrer des données avec une clé inconnue *câblée* dans le matériel; de plus, nous ne disposons pas du matériel nécessaire pour récupérer *physiquement* la clé dans le boîtier. Il nous est cependant possible de produire au moyen de textes clairs choisis les textes chiffrés correspondants avec cette clé inconnue.

La meilleure attaque différentielle connue demande actuellement 2^{47} textes clairs choisis. La phase d'analyse calcule la clé à l'aide de cet énorme amas de données. Une propriété intéressante de cette attaque est qu'il est possible de la monter même si le nombre de données disponibles est petit; la probabilité de succès augmente linéairement avec ce nombre.

Cryptanalyse linéaire

Une autre attaque théorique importante est la cryptanalyse linéaire. Elle a été proposée par Matsui, de Mitsubishi Electronics, en 1993 [6]. Bien qu'elle ne soit que théoriquement utile dans le monde réel, c'est l'attaque la plus efficace connue à ce jour contre DES.

Imaginons le scénario suivant: nous disposons d'un grand nombre de couples texte clair - texte chiffré avec une clé identique. Nous pouvons dans ce cas procéder à ce que l'on nomme une *attaque à texte clair connu*.

Ainsi, il est possible d'exploiter une faiblesse d'une des briques composantes de DES en effectuant des statistiques sur un flot de 2^{43} couples de données (soit la bagatelle de deux fois 64 To).

Projet actuel au LASEC

Un des projets actuels du LASEC (Laboratoire de Sécurité et de Cryptographie), est de mettre en œuvre cette attaque en analysant plus précisément son coût. Actuellement, cette attaque tourne sur une quinzaine de PC (certains prêtés gracieusement par le LTHI, le LTHC et par le LTS) et casse une clé tous les 4 à 5 jours. Elle emploie une implémentation de DES extrêmement rapide, développée et optimisée spécialement pour l'occasion, qui est capable de chiffrer des données à un taux de 192 Mbps sur un Intel Pentium III cadencé à 666MHz. Les premiers résultats théoriques ont démontré que l'attaque a une complexité moindre que celle estimée par Matsui, faits confirmés par les résultats expérimentaux.

Conclusion

Nous avons présenté de façon succincte six possibilités différentes de casser DES. Elles démontrent que cet algorithme est en fin de vie, et qu'on ne peut plus le mettre en œuvre pour protéger des données sensibles. Les autorités américaines l'ont bien compris, le processus d'adoption du prochain standard étant en passe d'aboutir ces prochains temps.

Références

[1] **Data Encryption Standard**, in Federal Information Processing Standards Publications, No. 46, U.S Department of Commerce, National Bureau of Standards, January 1977

[2] **Cracking DES**, Electronic Frontier Fundation, May 1998, O'reilly

[3] ***http://www.distributed.net/***

[4] M. Hellman, **A cryptanalytic time-memory tradeoff**, IEEE Transactions on Information Theory, v. 26, n.4, Jul. 1980, pp 401-406

[5] E. Biham and A. Shamir, **Differential Cryptanalysis of DES**, Springer-Verlag, 1993

[6] M. Matsui, **Linear Cryptanalysis of DES cipher**, Advances in Cryptology – EUROCRYPT '93 Proceedings, Springer-Verlag, 1994, pp. 386-397

[7] ***http://www.nsa.gov*** ■