TD8 – Sécurité et protocoles cryptographiques (1ère partie)

{Emmanuel.Godard, Yann.Esposito}@lif.univ-mrs.fr

24 novembre 2005

☞ Le but de ce TD va être de se familiarisé avec les systèmes de sécurité.

1 Protection standard

1.1. Rappelez comment protéger un réseau avec un pare-feu

(a) Quelle est l'efficacité d'un tel système, à quelles attaques est-ce sensible ?

1.2. Qu'est-ce qu'un pot de miel ?

(a) Quels sont les risques liés à l'installation d'un pot de miel ?

(b) Quelle configuration devrait-on alors adopter ?

2 Attaque par recherche exhaustive (brute force)

☞ En 1999, un groupe de cryptographiste on construit un craqueur de DES. Il était capable de tester les 2^{56} clés de DES en 56 heures. La machine coûtait 250 k$.

2.1. En extrapolant la loi de Moore. Combien de temps faudrait-il aujourd'hui à une machine similaire pour casser une clé DES ?

☞ MD5 est une fonction de hachage. Récemment, on a pu montrer que l'on pouvait calculer des collision. Une chercheuse déclarait même qu'elle arrivait à trouver des collision à la main.
Aussi, d'autres fonctions de hachages existent ; nottamment SHA-1. SHA-1 produit des "hash" de 160 bits. La probabilité de trouver une collision de SHA-1 au hasard est de 1 sur 2^{80} exactement. Si vous hachez 2^{80} messages, vous êtes sûr de trouver au moins une paire ayant le même "hash".

2.2. Combien de temps faudrait-il théoriquement pour trouver une collision de SHA-1 en utilisant une machine capable de générer 2^{69} "hash" en 56 heures. Sachant que l'on pourrait construire aujourd'hui un tel ordinateur qui coûterait entre 25 et 38 millions de dollars ?

2.3. Vous semble-t-il raisonnable d'utiliser SHA-1 comme fonction de hachage aujourd'hui ? Pour combien de temps ?

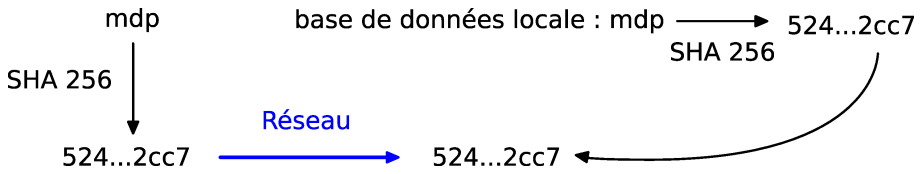
3 Protocoles

Commentez et critiquez les protocoles suivants (description, vulnérabilités, contexte d'utilisation)

3.1. Soit la méthode de chiffrement simple et robuste suivante :
- C_0 est la clé de session
- $C_i = M_i \oplus C_{i-1}$

3.2.

3.3.



3.4.

$$A \to S : r_{Ak}$$
$$S \to B : Aveutcommuniquer$$
$$B \to S : r_{Bk}$$
$$S \to A : r_B \oplus r_A$$