Rezumat temă licenţă

Algoritmi de criptare şi vulnerabilităţi

Pentru această temă mi-am propus să compar câţiva algoritmi hash şi să implementez unul sau mai mulţi algoritmi de tip block. Am ales să implementez algoritmi hash cum ar fi SHA pe 256 sau 512 biţi sau MD5. Un algoritm de tip hash reprezintă un algoritm matematic care aplicat pe orice şir de caractere va rezulta un alt şir de caractere de o dimensiune standard şi care va furniza un rezultat unic pentru fiecare şir de caractere. Acest tip de criptare se mai numeşte şi one-way deoarece algoritmul asigură doar criptarea şirului de caractere, nu şi decriptarea sa. Aceste sisteme sunt implementate în primul rând la stocarea parolelor pentru a fi ascunse de orice om care are acces la aplicaţie. Aceste chei hash se mai folosesc şi de către producătorii de software care includ pe lângă fişierul binar care reprezintă programul şi hash-ul acestuia. Astfel după ce se downloadează fişierul, se calculează hash-ul acestuia apoi se compară cu cel afişat pe site-ul producătorului. Dacă hash-urile nu sunt identice atunci fişierul a fost modificat. Un singur bit modificat în informaţia a cărui hash calculam generează un Diggest complet diferit.

O scurtă prezentare a algoritmilor hash mai sus menţionat poate fi:

1. MD5 - Message Diggest Version 5

- generează un hash pe 128 biţi exprimat în 32 cifre hexazecimale;

- a fost creat de prof. Ronald Rivest de la MIT în 1991;

- a fost standardizat în RFC1321;

- este unul dintre cei mai folosiţi algoritmi de hashing în prezent (2009);

- începând cu anul 2004 au început să fie descoperite diferite vulnerabilităţi în algoritm multe ne-fatale. Se consideră că va fi înlocuit în curând de alt algoritm mai sigur;

2. SHA1 - Secure Hash Algorithm Version 1

generează un hash output pe 160 biţi exprimat în 40 cifre hexazecimale;

- a fost creat şi publicat de guvernul UŞĂ (NSA) în 1993;

- operează pe mesaje de maximum 2^64-1 biţi;

- este unul dintre cei mai folosiţi algoritmi de hashing în prezent (2009);

- începând cu anul 2004 au început să fie descoperite diferite vulnerabilităţi în algoritm multe

ne-fatale. Se consideră că va fi înlocuit în curând de alt algoritm mai sigur;

- SHA2 este o nouă familie de algoritmi de Hash publicați în 2001 care conține SHA-224, SHA-256, SHA-384 și SHA-512 după nr. de biți ai outputului;

- SHA3 reprezintă un nou protocol care este încă în dezvoltare și va fi supus unei competiții publice după 2012;

Acești algoritmi, după cum am menționat mai sus sunt ireversibili, tocmai de aceea oamenii care au avut plăcerea de a descifra o anumită cheie, au inventat diverși algoritmi care vor sparge sau nu o anumită cheie. Voi prezenta câțiva mai jos:

1. Collision attack

Presupune găsirea a două mesaje oarecare cu același hash în mai puțin de 2^(L/2) iterații. Acest tip de vulnerabilitate nu reprezintă o problemă de securitate.

2. First pre-image attack

Presupune găsirea unui mesaj care determină un hash dat în mai puțin de 2^L iterații. Acest tip de vulnerabilitate reprezintă o gravă problemă de securitate.

3. Second pre-image attack

Presupune găsirea unui mesaj M2, având-se un mesaj M1 care să determine același hash în mai puțin de 2^L iterații. Acest tip de vulnerabilitate reprezintă o gravă problemă de securitate.

L = lungimea hash-ului rezultat

Am ales această temă deoarece prezintă un interes destul de ridicat modul în care securitatea este menținută în zilele noastre și modul în care oamenii luptă din 2 direcții, unii pentru a o face cât mai sigură, iar alții pentru a demonstra că nu totul este atât de sigur pe cât pare. Mi-am propus să expun în linii mari această viziune a securității și câțiva timpi demonstrativi în care o cheie implementată cu diferiți algoritmi va fi decriptată în timpi semnificativ diferiți.