Lunghezza della chiave e protezione dei dati

Leonardo Miliani | 13 aprile 2007

Quante volte, in ambito informatico, sentiamo fare riferimento alla lunghezza della chiave come ad un fattore importante per la sicurezza? Molte volte, penso. L'utilizzo più frequente è nella frase "protezione con chiave a xxxx bit", intendendo con essa che un qualche documento è protetto con un algoritmo che utilizza una chiave di cifratura la cui lunghezza è xxxx bit*.

Ma sapere questo valore ha qualche… valore? Chi non è pratico di algoritmi crittografici può capire il reale livello di protezione che xxxx bit offrono ai suoi dati o documenti? E perché una chiave pubblica deve essere molto più lunga di una chiave privata? E quanto possono rimanere protetti i miei dati con una chiave a xxxx bit? A queste ed altre domande cercherò di dare una risposta al tempo stesso semplice ma esaustiva.

Torniamo per un attimo indietro nel tempo, alla metà degli anni '70, quando il Governo Americano introdusse il **DES** (Data Encryption Standard), un algoritmo di cifratura a **56 bit** derivato dal Lucifer di IBM ed adottato come standard per la protezione dei documenti sensibili. All'epoca della sua adozione (il Lucifer è del 1974, il DES viene presentato nel 1975 ed adottato nel 1977), i 128 bit dell'ultima versione del Lucifer vennero ritenuti inutili dato che le prestazioni dell'hardware del periodo non erano entusiasmanti. Si decise perciò che il DES avrebbe avuto una chiave di soli 56 bit, questo per ridurre i tempi di cifratura/decifratura dei documenti tanto la potenza elaborativa dei computer di allora non avrebbe mai permesso di violare un documento protetto con il DES in un tempo accettabile. Da quel lontano 1977 il DES visse un ventennio di gloria, durante il quale per ben 3 volte fu riconfermato come lo standard per i documenti del Governo Americano.

Bisogna infatti arrivare al 1997 per avere la prima violazione di un documento cifrato con il DES: il progetto DESCHALL riuscì nell'impresa dopo 96 giorni di elaborazione dei dati! Ma l'hardware in quegli anni faceva passi da gigante: così, già nel 1998 l'EFF DES Cracker, una macchina con 1800 CPU integrate poteva violare il DES in sole 56 ore. E nel 1999 una versione migliorata dell'EFF effettuava l'operazione in 22 ore e 15. Il Governo Americano capì subito che le cose andavano male per il vecchio DES ed introdusse prima il **TripleDES**, una versione a 112 bit del vetusto algoritmo, e poi, nel 2002, adottò come standard un nuovo algoritmo, il famoso **AES**, che può operare con chiavi a 128 e 256 bit.

Dopo questo tuffo nel passato,vediamo di entrare nei dettagli e capire su cosa si riflette la lunghezza di una chiave e perché un algoritmo con una chiave di poche decine di bit è considerata inadeguata per i computer odierni. Fino a pochi anni fa i più diffusi algoritmi di cifratura a chiave simmetrica (cioè nei quali la stessa chiave serve sia per cifrare che per decifrare i dati) erano tutti "a blocchi": in essi l'algoritmo di cifratura opera su porzioni di dati (definite blocchi) e, mediante una serie di operazioni più o meno complesse, interpola la porzione di dati con la chiave di cifratura per ottenere un blocco di dati cifrati. E' ovvio che più la chiave di cifratura è lunga minore è la frequenza con cui i suoi singoli elementi vengono riutilizzati e, conseguentemente, minore è la possibilità che i dati cifrati portino con sé informazioni capaci di aiutare un pirata informatico a ricostruire la chiave. Inoltre, più corta è la chiave e più è facile forzare il documento cifrato ricorrendo al già menzionato **attacco a forza bruta**, dove un software prova tutte le combinazioni di caratteri possibili date dalla lunghezza della chiave stessa: il massimo numero di chiavi è dato da ***2^lun_chiave*** in bit, nel caso del DES da 2^56 = più di 72 miliardi di miliardi di chiavi. Il numero sembra elevato ma la macchina che violò il DES nel 1999 in 22 ore compiva più di 320 milioni di miliardi di test all'ora!

Abbiamo citato l'AES e la sua struttura che può operare su chiavi a 128 e 256 bit. Ricordando la formula *2^lun_chiave*, vediamo che le possibili combinazioni crescono in maniera vertiginosa al

crescere di *lun_chiave* e già con una chiave a 128 bit possiamo dormire sonni (relativamente) tranquilli: la mia calcolatrice scientifica ha detto che le possibili combinazioni sono 3,4028e+38, vale a dire 3 seguito da 38 zeri! Ecco perché il DES non viene più considerato sicuro!

Ma non devono essere usati neanche algoritmi con chiavi inferiori ai 128 bit se il livello di sicurezza che cerchiamo deve essere molto elevato. Stando, infatti, al documento che annualmente l'ECRYPT (il consorzio europeo per la crittografia) pubblica sulla lunghezza delle chiavi consigliate, per ottenere ad oggi una protezione sicura contro gli attacchi più diffusi bisogna usare una chiave di almeno 80 bit; ma se vogliamo conservare i nostri dati per molti anni (diciamo oltre i 20) allora i 128 bit sono assolutamente necessari.

Un altro punto fondamentale che finora abbiamo tralasciato è il tipo di algoritmo utilizzato. Fino a questo momento tutte le nostre congetture si basavano sull'utilizzo di un algoritmo di cifratura con chiave simmetrica, vale a dire dove la stessa chiave si utilizza sia per cifrare che per decifrare i dati e la cui sicurezza si basa sul rendere inaccessibile a tutti la chiave. Ma nel caso di uno scambio di dati via e-mail fra 2 persone che non si possono incontrare di persona per scambiarsi una chiave simmetrica? In questo caso si utilizza un algoritmo di cifratura a **chiave pubblica** (per i dettagli, vi rimando ad un mio precedente articolo), dove la chiave pubblica (o chiave asimmetrica, perché si può usare solo per un'operazione, quella di cifratura) può essere appunto distribuita senza problemi dato che solo chi è in possesso della chiave di decifratura (definita privata) potrà leggere quei dati. Ma per offrire un elevato livello di protezione, questa chiave deve essere necessariamente più lunga di una chiave simmetrica. Di quanto, però?

Stando alle ricerche degli specialisti, per offrire la protezione offerta da una chiave simmetrica ad 80 bit una chiave RSA (un famoso algoritmo a chiave pubblica) deve essere lunga 1248 bit; per avere la protezione offerta da una chiave simmetrica a 128 bit bisogna salire a 3248 bit; per avere invece la protezione offerta da una chiave a 256 bit dobbiamo addirittura utilizzare una chiave pubblica di ben 15424 bit! Capite quindi che le chiavi pubbliche di soli 512 bit, corrispondenti ad una chiave simmetrica di appena 50 bit, sono assolutamente inefficaci per proteggere i dati più sensibili! Anche le chiavi pubbliche a 1024 bit, le più diffuse, offrono la protezione di una chiave simmetrica da 73 bit (queste ultime sono, oggigiorno, violabili in veramente pochi giorni di calcolo). Meglio utilizzare chiavi pubbliche di almeno 2048 bit (un taglio abbastanza diffuso) per avere una protezione paragonabile a quella offerta da una chiave simmetrica a 103 bit. Ma se volete dormire sonni tranquilli allora il consiglio è di utilizzare, dove possibile, una chiave pubblica da 4096 bit.

Eccoci alle conclusioni: che lunghezza di chiave adottare, tenendo conto del rapporto protezione offerta/complessità di calcolo? Dipende, come detto, dal livello di sicurezza che uno ricerca:

- se il livello è minimo e serve solo una protezione a brevissimo periodo allora è sufficiente utilizzare una chiave di lunghezza inferiore ai 64 bit;
- se si devono proteggere dei dati per brevi periodi e solo contro l'attacco di singoli individui o piccole società allora si può adottare una chiave a 72 bit;
- per avere una protezione garantita per un paio di anni la lunghezza minima della chiave deve essere di 80 bit;
- una chiave a 96 bit è prevedibile che offra una protezione non superiore ai 10 anni;
- per una protezione di 20 anni si deve utilizzare una chiave di almeno 112 bit ;
- dati estremamente sensibili o che devono resistere per almeno 30 anni devono essere protetti con una chiave non inferiore ai 128 bit;
- la protezione offerta dalle chiavi a 256 bit che alcuni algoritmi permettono di utilizzare si può definita, allo stato attuale della tecnica, "da qui all'eternità".

Per approfondire il concetto di sicurezza informatica, rimando a questo mio articolo.

* per i meno ferrati in informatica:
un bit è l'elemento più piccolo immagazzinabile in un computer e corrisponde ad una singola cella di memoria che può assumere 2 valori definiti: 0 oppure 1; 8 bit costituiscono il byte, il gruppo di dati più piccolo che generalmente viene preso in considerazione. Il byte è anche la più piccola unità indirizzabile da un calcolatore, definita spesso "locazione di memoria". Anche se i bit sono in realtà l'unità fondamentale, i processori utilizzano i byte per immagazzinare le informazioni. 1 byte, cioè 8 bit, possono immagazzinare un numero intero che va da 0 a 255, di solito utilizzato per rappresentare un carattere di testo. Quindi, una chiave a 128 bit possiamo a grandi linee paragonarla ad una sequenza di 128/8=16 caratteri).

P.S.:
articolo pubblicato sulla rivista Hakin9.