La crittografia a chiavi pubbliche è a rischio?

Il mondo della sicurezza informatica è a rumore e vi sono molte discussioni fra esperti ed appassionati sullo stato della crittografia a chiave pubblica; la domanda più pressante è se è ancora sicuro utilizzare protocolli quali l'RSA. Cercherò qui di fare il punto della situazione e dare qualche informazione che aiuti a capire quello che sta succedendo.

Io scorso novembre, il Professor Daniel Bernstein dell'Università dell'Illinois (Chicago), pubblicò un articolo scientifico (reperibile all'indirizzo http://cr.yp.to/papers.html#nfscircuit) in cui proponeva dei miglioramenti all'algoritmo usato per trovare i numeri primi, cioè non divisibili per altri numeri interi, divisori di un grande numero intero. La "fattorizzazione in numeri primi di un numero intero" è un difficile problema matematico per il quale non si conosce alcun algoritmo efficiente quando il numero intero da fattorizzare è grande, ed anzi più il numero è grande più l'algoritmo è lento, in modo esponenziale. La maggior parte dei protocolli di crittografia a chiave pubblica, come il famoso RSA, sono basati sul fatto che con i computer attuali la fattorizzazione di un grande numero intero può richiedere tempi in media anche dell'ordine di migliaia di anni. La crittografia a chiave pubblica è utilizzata in molti tra i protocolli crittografici di maggior uso, come ad esempio https, ssh, IPSec, s/mime, pgp etc..

Con il suo articolo Bernstein in realtà proponeva alla National Science Foundation americana di finanziare una ricerca per stabilire quanto più velocemente si possano fattorizzare i numeri primi utilizzando le modifiche da lui proposte. E' da notare che si tratta solamente di miglioramenti agli algoritmi noti, e non di un nuovo algoritmo che permette di decifrare facilmente, ad esempio, tutte le chiavi RSA. (In termini più tecnici, non cambia l'andamento esponenziale nel numero di bit della chiave del "costo" richiesto per la decifrazione, si ridurrebbe solamente l'esponente.) Inoltre la proposta di Bernstein richiede la costruzione di circuiti appositi, possibile con le attuali tecnologie, ma dal costo odierno dell'ordine delle centinaia di milioni se non miliardi di dollari.

Con l'algoritmo tradizionale di fattorizzazione è stata decifrata recentemente una chiave RSA a 512 bit in 6 settimane utilizzando una rete di computer commerciali da ufficio (comunicazione a "Financial Cryptography 2002" di Nicko van Someren, nCipher

Inc.,UK). Pertanto le chiavi simmetriche a 512 bit sono oggi considerate non sicure. Con l'algoritmo tradizionale le chiavi a 1024 bit sono però ancora sicure, ovvero non decifrabili in un tempo ragionevole con alcun computer esistente ora o nel prossimo futuro. Se i miglioramenti proposti da Bernstein all'algoritmo di fattorizzazione si rivelassero efficienti, le stime più pessimistiche indicano che le chiavi a 1024 bit potrebbero essere decifrate in qualche minuto o decina di secondi, utilizzando l'hardware costruito appositamente. Le chiavi RSA a 2048 bit sarebbero però ancora sicure per molti anni, anche tenendo conto della legge di Moore secondo cui la velocità dei computer raddoppia ogni 18 mesi.

In ogni caso questi sviluppi non sono inaspettati. Ad esempio già nel 1995 Bruce Schneier in "*Applied Cryptography"* prevedeva che nell'anno 2000 le più brevi chiavi RSA considerate sicure sarebbero state a 1024 bit, e nel 2005 a 1280 bit. Suggeriva inoltre a chi avesse particolari esigenze di sicurezza, di utilizzare a partire dal 2005 chiavi non inferiori a 2048 bit.

Quali conseguenze possono avere per le applicazioni pratiche di sicurezza informatica questi risultati? Le opinioni sono molto discordanti, posso però fare qui qualche osservazione. In primo luogo sono ben pochi i sistemi di sicurezza informatica ove l'anello debole è dato dalla lunghezza della chiave a crittografia pubblica, anche se essa è a 512 bit. I maggiori problemi sono di solito dati da vulnerabilità nel software (anche crittografico), ed errate progettazioni, implementazioni o gestioni dei sistemi di sicurezza. Una seconda osservazione è che i software crittografici attualmente in commercio, e penso ad esempio ai browser web con SSL, raramente permettono all'utente o all'amministratore di richiedere che le chiavi crittografiche utilizzate non siano inferiori ad un certo numero di bit. Alla luce di quanto detto, questa possibilità diventerà alquanto importante nel prossimo futuro. Infine va ricordato che non vi è la certezza matematica che non esista un algoritmo "veloce" per la fattorizzazione dei numeri interi, in termini matematici non è stato dimostrato che un problema "NP−HARD" non ammette una soluzione "P". Pertanto vi è una piccolissima possibilità che qualcuno scopra un algoritmo "veloce" che renda del tutto insicura la crittografia basata sulla fattorizzazione in numeri primi. Inoltre vi è la possibilità che un giorno i "Quantum Computers" diventino realtà e siano in grado di fattorizzare qualunque numero intero in pochi secondi. Queste possibilità sembrano però molto lontane nel futuro, e quindi praticamente trascurabili nelle

applicazioni pratiche di oggi.

Per quanto riguarda la lunghezza delle chiavi a crittografia pubblica da utilizzare, se si sta progettando un sistema di sicurezza informatica è bene partire con chiavi a 1024 bit tenendo conto che, fra un paio di anni, potrebbe essere necessario fare un aggiornamento a chiavi tra i 1280 e 2048 bit. Poiché il "costo" di utilizzo di una chiave crittografica cresce linearmente, ma con un fattore 6 o 7, con il numero di bit, il sistema deve essere progettato in modo da poter "scalare" facilmente. Per i sistemi già esistenti se si utilizzano chiavi di lunghezza inferiore a 1024 bit, il consiglio è di pensare seriamente ad aggiornare il sistema per utilizzare chiavi a 1024 bit entro i prossimi 10 mesi ed in questo caso prevedere già la possibilità di salire a 1280 o più bit nei prossimi 2 o 3 anni. La decisione dipende ovviamente dal costo globale dell'aggiornamento, sia per quanto riguarda l'hardware ma anche, ad esempio, le possibili conseguenze psicologico−pubblicitarie dell'uso di chiavi considerate insicure in una applicazione di commercio elettronico. Infine se la vostra richiesta di sicurezza è "assoluta", come ad esempio per applicazioni militari, il suggerimento è di usare chiavi a 2048 o 4096 bit.

Andrea Pasquinucci
Consulente di Sicurezza Informatica
pasquinucci@ucci.it

Anno	***Personale***	***Aziendale***	***Governativo***
1995	768	1280	1536
2000	1024	1280	1536
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

Lunghezza minima (in bits) delle chiavi RSA per uso Personale, Aziendale e Governativo consigliata da Bruce Schneier in *Applied Cryptography,* 1995.