Numeri casuali e sicurezza informatica

Come ogni anno da otto anni a questa parte la società di password management **SplashData** ci ricorda con impietosa puntualità la nostra totale fiducia nel prossimo; oppure, messa in altri termini, la nostra totale mancanza di fantasia.

Se leggiamo con sguardo naive la lista delle password più usate nel 2018 e non è che le cose siano migliorate più di tanto rispetto agli anni precedenti, ci accorgiamo della nostra totale ingenuità nei confronti delle più normali norme di sicurezza; a partire proprio dalla password che deve essere come abbiamo già ricordato in un nostro precedente post:

- facile da ricordare
- difficile da indovinare

Il primo criterio è ampiamente rispettato, come ci ricorda la classifica stilata da SplashData; visto che ai primi tre posti figurano le combinazioni numeriche ***123456***, quella alfabetica con la parola ***password*** e la sequenza ***123456789*** (per quelli che alla sicurezza ci tengono davvero).

Il secondo aspetto per una crittografia se non a prova di hacker, perlomeno in grado di offrire un qualche margine di protezione, viene ampiamente ignorato con addirittura la sequenza terza classificata che ha scalato ben due posizioni rispetto al 2017. Potrebbe anche non essere un campione rappresentativo della maggioranza degli utenti globali, dato che la classifica ha preso in esame esclusivamente un paniere di cui fanno parte utenti americani ed europei. Ma il problema della vulnerabilità resta comunque una faccenda seria e di questo si occupano le varie piattaforme, suggerendo ai propri utenti sequenze alfanumeriche con un elevato livello di sicurezza e vari laboratori in giro per il mondo.

E veniamo allora al problema della casualità nella scelta delle stringhe di numeri che stanno dietro agli attuali sistemi crittografici. Una casualità tutt'altro che assoluta o se vogliamo reale. Alla base di ogni sistema in grado di produrre sequenze di numeri troviamo infatti dei semi, ***seed***, che rappresentano la sorgente che dà avvio alla sequenza. Questa sorgente indica all'algoritmo i numeri da scegliere, ad esempio tra 0 e 100.

Il paniere scelto potrebbe essere ancora più ampio e prendere in considerazione sequenze di numeri primi molto grandi, ma in entrambi i casi la scelta sarà determinata dal seed. Vale a dire da un intervento umano, determinato anche se nel caso dei numeri primi difficilmente scardinabile con le macchine attuali.

Da anni i ricercatori sono impegnati nello sviluppo di algoritmi in grado di generare i cosiddetti **TRNG**, numeri veramente casuali (*true random number generator*). Una necessità fondamentale in una società in cui mail, transazioni bancarie, la nostra stessa privacy dipendono dall'impenetrabilità di questi sistemi.

La questione della ricerca di generatori di numeri davvero casuali non è storia recente; ad occuparsene infatti nel corso dei secoli incontriamo personaggi bizzarri che hanno scelto i più improbabili laboratori per scovare generatori di numeri casuali realmente efficienti e a prova di determinismo. Nei primi anni del Novecento in quel di Montecarlo incontriamo ad esempio il **matematico Karl Pearson** che per trovare un sistema di riferimento per i suoi studi sulle sequenze numeriche casuali scelse i tavoli della roulette. Le cose non andarono molto bene; dopo un mese di studio si accorse che le serie di numeri uscite sui bollettini periodici non erano affatto casuali, ma venivano inventate di sana pianta dai giornalisti incaricati di redigerle.

Una conferma in più di quanto l'essere umano non sia in grado

di elaborare, alla lunga, sequenze di numeri davvero casuali.

Diverso invece l'approccio adottato nel 2010 dai ricercatori della **Queen's University a Belfast** che hanno sviluppato una macchina più piccola delle versioni precedenti e con un peso del 50% inferiore capace di sfruttare il rumore bianco per la generazione di numeri veramente casuali.

Altra linea di ricerca quella seguita nel 2017 dal team dell'**Università di Ginevra**, coordinato dal professor Nicolas Brunner che ha basato il proprio sistema sui principi della fisica quantistica.

L'impossibilità di predeterminare un risultato all'interno di un sistema quantistico, un esempio classico è quello dello **spin dell'elettrone**, apre la strada a esperimenti come quello avvenuto a Ginevra dove i ricercatori hanno impiegato un laser per sparare fotoni contro un vetro semitrasparente. La particella di luce si comporterà in due modi: o passerà attraverso la superficie oppure ne verrà riflessa. Impossibile stabilire a priori uno dei due risultati. È sulla base di questo principio che presto potremo contare su macchine in grado di generare numeri davvero casuali. Non proprio tascabili al momento visto che il sistema è grande quanto una stanza.

Ma già le dimensioni si stanno riducendo, se non altro rispetto agli attuali computer quantistici che come il **Q System One** della IBM è stato presentato lo scorso Gennaio al CES di Las Vegas. Il primo modello di computer quantistico per uso commerciale. Non proprio uno smartphone, ma apre comunque la strada al futuro di generatori di numeri casuali davvero efficaci e forse presto alla portata di tutti.

https://www.ictsecuritymagazine.com/notizie/numeri-casuali-e-sicurezza-informatica/