Google dà la mazzata finale all'algoritmo crittografico SHA1

Google ha finalmente crackato l'agoritmo SHA1, utilizzato come funzione di hashing per verificare l'attendibilità di un file o identificare eventuali modifiche forzate

di Nino Grasso pubblicata il **24 Febbraio 2017**, alle **14:31** nel canale Sicurezza
Google

L'algoritmo crittografico **SHA1 (Secure Hash Algorithm 1)** è adesso considerabile inutile, morto sotto l'ultimo colpo inferto da Google. Big G ha riportato il **primo attacco avvenuto con successo per portare a compimento una *collisione hash* fra due file protetti dalla crittografia mediante SHA1**. La tecnologia dovrebbe infatti generare hash unici per ogni serie di dati per identificare ciascun file con un identificativo. Quello che ha dimostrato Google è che, nella pratica e non solo nella teoria, due file diversi possono essere contrassegnati con lo stesso hash.

La funzione **SHA1** è stata progettata dalla National Security Agency (la famosa NSA) americana e l'algoritmo è stato reso pubblico nel 1995. Già nel 2005 alcuni cripto-analisti avevano messo in dubbio la sua efficacia e annunciato alcune falle che in via teorica avrebbero potuto essere sfruttate via *"collision hash"*. Una pratica estremamente pericolosa se si considera che in questo modo file malevoli potrebbero essere scambiati per file del tutto legittimi senza lasciare alcuna traccia, dando via libera quindi ad un potenziale aggressore che potrebbe iniettare malware sul computer vittima.

Un altro duro colpo alla tecnologia è stato inferto di recente, quando nel 2015 un gruppo di ricercatori di diverse università del mondo hanno collaborato per redigere il documento noto come ***The SHAppening***, in cui in linea di massima si consigliava di passare alle più moderne ed efficaci tecnologie SHA2 e SHA3 abbandonando del tutto SHA1 per la potenziale vulnerabilità agli attacchi "collision hash". Gli scienziati all'occorrenza avevano dimostrato che la maggiore potenza dei computer odierni può rappresentare un forte pericolo per i file protetti con SHA1.

Stando al documento con un investimento fra i 75.000 e i 120.000 dollari chiunque avrebbe potuto **crackare SHA1 utilizzando il servizio EC2 di Amazon** (di cloud computing), una cifra che diversi governi e realtà aziendali possono investire senza troppi patimenti. Una volta che la potenziale vulnerabilità è divenuta pubblica parecchi produttori di browser (Mozilla, Microsoft, Google) hanno iniziato ad **abbandonare rapidamente SHA1** come funzione di hashing per i certificati TLS/SSL, ampiamente utilizzati sul web fra le soluzioni di crittografia.

Da allora Google ha contattato due dei ricercatori coinvolti nel progetto The SHAppening e ha offerto la propria collaborazione e l'enorme potenza di calcolo in cloud di cui dispone per continuare il lavoro, al fine di ottenere una prova pratica di quanto dimostrato teoricamente fino ad oggi. Un team composto complessivamente da sette uomini ha infine pubblicato una nuova ricerca che spiega le caratteristiche di un attacco "collision hash" realmente avvenuto. Come prova del successo dell'esperimento sono stati rilasciati **due file PDF diversi con lo stesso hash SHA1**.

Per intuire l'entità della problematica vi proponiamo l'esempio di un documento importante, magari un accordo di lavoro, salvato online come PDF e protetto attraverso hash SHA1 per identificarlo come unico e attendibile, e per dimostrare che nessuno lo ha modificato dopo la stipulazione. Adesso che si ha la **certezza comprovata che SHA1 non è più attendibile**, lo stesso metodo non può più essere considerato valido dal momento che non si può più offrire la certezza che non sia stato modificato dopo l'ultima interazione legittima con il documento.

Bisogna tuttavia fare una precisazione importante: per effettuare l'attacco Google ha dovuto organizzare, stando ai propri stessi annunci, "uno dei più grandi calcoli computazionali mai portati a termine". Sembra quindi economicamente molto difficile che l'attacco possa essere effettuato se non da enti enormi, come ad esempio governi o società che possono affidarsi a grossi sistemi o servizi in cloud. Google rilascerà un codice "proof-of-concept" con le modalità di esecuzione dell'attacco nei prossimi 90 giorni, dopo i quali sarebbe meglio abbandonare del tutto SHA1. Senza se e senza ma.