Una sicurezza quantistica

Un Internet quantistico in grado di inviare messaggi perfettamente sicuri è stato realizzato e messo in esercizio nei laboratori governativi di Los Alamos da due anni e mezzo.

The Physics arXiv Blog

Uno dei sogni degli esperti di sicurezza è la creazione di un Internet quantistico che permetta una comunicazione perfettamente sicura, basato sulle leggi potenti della meccanica quantistica. L'idea di base è che l'atto di misurare un oggetto quantistico, come un fotone, cambia sempre lo stesso oggetto. Quindi ogni tentativo di intercettare un messaggio quantistico non può non lasciare segni rivelatori. Ciò permette a chiunque di inviare un *one-time pad* su una rete quantistica, che può venire utilizzato per comunicare in sicurezza con le modalità convenzionali.

Questo metodo consente una messaggistica perfettamente sicura, nota come crittografia quantistica ed è alla portata di qualsiasi decente laboratorio di ottica quantistica. In effetti, l'azienda ID Quantique commercializza un sistema *off-the-shelf*, che sta attirando le banche e altre organizzazioni interessate a una sicurezza perfetta.

Tuttavia, l'attuale generazione di sistemi di crittografia quantistica si basa su connessioni punto-a-punto realizzate mediante una singola fibra, così che si possono inviare messaggi sicuri tra A e B, ma non instradare queste informazioni a C, D, E o F. L'instradamento di un messaggio, infatti, comporta che ne venga letta la parte indicante dove deve venire instradato e ciò altera il messaggio, rendendo impossibile un Internet quantistico realizzato con le odierne tecnologie.

Vari gruppi di ricerca stanno cercando di sviluppare router quantistici che possano risolvere questo problema gestendo messaggi quantistici senza alterarli.

Oggi, Richard Hughes e i suoi collaboratori dei Laboratori governativi di Los Alamos nel New Mexico danno notizia di un Internet quantistico alternativo, che sarebbe stato utilizzato da oltre due anni. Il loro approccio comporta la creazione di una rete quantistica basata su un hub e su una rete di tipo vocale. Tutti i messaggi vengono instradati da qualsiasi punto della rete a un altro attraverso questo hub centrale. L'idea è che i messaggi che passano per l'hub godano di un livello di sicurezza quantico.

Fintanto che l'hub è sicuro, la rete sarebbe sicura. Ma il problema di questo approccio è la scalabilità. Poiché il numero di link all'hub aumenta, diventano sempre più difficili da gestire tutte le possibili connessioni. Hughes sostiene di avere risolto questo problema equipaggiando ogni nodo della rete con trasmittenti quantistiche, cioè con laser, ma non con i rivelatori di fotoni, che sono costosi e ingombranti. Solo l'hub è in grado di ricevere un messaggio quantistico (sebbene tutti i nodi possano inviare e ricevere messaggi convenzionali in modo normale). Questo metodo permette d'inviare da ogni nodo un *one-time pad* all'hub, che può quindi inoltrare questo messaggio a un altro nodo utilizzando un secondo *one-time pad*. Così l'intera rete è sicura, a condizione che l'hub centrale sia sicuro. Il grande vantaggio è che la tecnologia necessaria a ogni nodo viene resa estremamente semplice, essenzialmente poco più di un laser. In effetti, Los Alamos ha già realizzato moduli *plug-and-play* che hanno le dimensioni di una scatola di fiammiferi: «Il modulo di prossima generazione sarà di un ordine di grandezza più piccolo in ogni dimensione».

L'obiettivo è quello di inserire uno di questi moduli in ogni dispositivo collegato a una rete in fibra ottica, dai *set top box* televisivi ai computer domestici, per permettere una messaggistica perfettamente sicura. ■

Una sicurezza all'insaputa

Alcuni ricercatori stanno lavorando a password talmente segrete da essere conosciute solamente dalla parte non cosciente della mente.

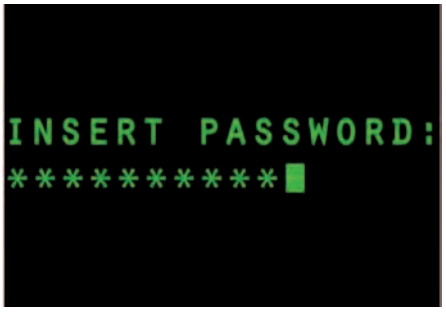
Rachel Metz

Alcuni sforzi, volti alla sostituzione delle password composte tradizionalmente da lettere e numeri, si affidano a movimenti del corpo, a dispositivi indossabili o alla biometria.

Un approccio diverso, attualmente in fase di studio da parte dell'azienda di ricerca e sviluppo SRI International e dalla Stanford and Northwestern, mira invece a una soluzione completamente differente: password che si conoscono, senza però sapere di conoscerle.

Patrick Lincoln, direttore del laboratorio di scienza informatica della SRI, definisce il progetto un "sistema di autenticazione a prova di tubo di gomma", facendo riferimento alla "crittoanalisi tramite tubo di gomma", in cui una persona viene costretta forzatamente a rivelare informazioni come la password d'accesso a un edificio protetto.

Secondo Lincoln, l'approccio farebbe affidamento sull'apprendimento implicito – quell'apprendimento che avviene ripetendo un'azione, come quando s'impara ad andare in bicicletta, senza spiegazioni verbali – per prevenire la compromissione di una password. Per ora, il progetto ha utilizzato l'interfaccia di un gioco, una versione rudimentale di Guitar Hero, attraverso cui si viene addestrati a seguire uno schema preciso. L'utente preme un comando, corrispondente a una colonna, ogni volta che una pallina tocca il fondo di una delle colonne, ma siccome la sequenza di palline in caduta varia in continuazione, l'utente non è in grado di distinguere consapevolmente la loro sequenza da altri segnali impropri. In seguito, l'utente è autenticato facendolo giocare a un gioco che contiene parti degli schemi memorizzati, che permettono di identificarlo.



Si tratta di uno dei tanti tentativi per abbandonare le password tradizionali, che possono essere difficili da ricordare e non sicure. Se i ricercatori riusciranno a perfezionare questo sistema, potrebbero agevolare l'accesso degli operatori ad aree dall'elevata sicurezza, come per esempio le cabine di pilotaggio degli aerei, oltre ad ambiti più diffusi, come i conti bancari. Gli utenti, inoltre, potrebbero riuscire ad apprendere più di una password inconscia senza alcuna interferenza, per cui sarebbe possibile avere una password per l'ufficio e un'altra per il conto in banca. Qualora una password venisse in qualche modo compromessa, se ne potrebbe apprendere un'altra senza cancellare la prima.

Le scoperte iniziali dei ricercatori sono state pubblicate lo scorso anno in un documento che include uno studio secondo cui gli utenti "addestrati" erano in grado di eseguire lo schema appreso senza esserne consapevoli. Il progetto ha ricevuto un premio dalla National Science Foundation che, a detta di Lincoln, sta permettendo di portare avanti le ricerche. Per ora, l'addestramento richiede circa 40 minuti per password e l'accuratezza del sistema necessita di miglioramenti. Il gruppo di Lincoln sta avviando nuovi esperimenti che dovrebbero portare a password inconsce più efficaci e facili da apprendere.

Nonostante le problematiche di un sistema del genere, David Wagner, docente di scienza dei computer presso la UC Berkeley ed esperto di sicurezza informatica, nota che anche altre tecnologie di sicurezza si stanno diffondendo malgrado le difficoltà iniziali, quale per esempio la crittografia tramite chiave pubblica, che ha avuto inizio negli anni Settanta con l'invenzione dell'algoritmo di codificazione RSA. «Almeno in teoria, è possibile disporre di una password da poter utilizzare senza esserne consapevoli». ■

Rachel Metz è redattrice di MIT Technology Review.

Una sicurezza tra le nuvole

Un modo per verificare se i dati sensibili sono stati manomessi potrebbe rendere il cloud computing più affidabile.

Tom Simonite

Oggi è normale che ogni genere di dati, dalle foto personali ai documenti societari, venga archiviato in server esterni. Ma nonostante la crescente utilizzazione di strutture esterne come la nuvola, non sembra crescere la fiducia sulla possibilità tecnologica di difendere davvero i propri dati. Come le irruzioni recenti su Twitter e Linkedin dimostrano, anche i servizi più accreditati non sono immuni da attacchi e questa è una grande sfida per le aziende che stanno cercando di esternalizzare le operazioni relative a dati sensibili.

Un software chiamato Pinocchio, creato dai ricercatori di IBM e Microsoft, fornisce una possibile soluzione, funzionando come una "macchina della verità" che può venire usata per controllare se un servizio cloud ha svolto il lavoro programmato, o se è stato costretto a fare qualcosa di diverso.

Il software potrebbe anche venire usato per migliorare la privacy, offrendo un modo affidabile di trattare i dati personali in remoto, piuttosto che nei server aziendali.

Pinocchio prende un gruppo di operazioni scritte nel linguaggio di programmazione C e le converte in una versione integrata nel codice. Questo nuovo gruppo viene inviato sul servizio cloud, per svolgere il lavoro programmato. La conversione produce una chiave di verifica che consente di controllare se i risultati sono veramente il frutto delle operazioni richieste.

«La chiave di verifica si comporta come una firma digitale, che si può fornire a ogni server esterno per controllare un risultato», spiega Bryan Parno, uno dei ricercatori della Microsoft impegnati su Pinocchio. Parno ha sviluppato Pinocchio con il collega della Microsoft Jon Howell, oltre che con Craig Gentry e Mariana Raykova dell'IBM.

Gentry è conosciuto per avere provato che è possibile, al servizio cloud, lavorare su dati criptati senza doverli decriptare, in modo da proteggere la sicurezza dei dati.

Parno sostiene che in questo momento il solo modo di conoscere con certezza se un provider cloud ha svolto il lavoro che gli era stato chiesto, è quello di eseguire nuovamente il lavoro. Le aziende possono evitare truffe o errori, controllando in modo casuale i risultati, o chiedendo a più provider di fare lo stesso lavoro. Ma questo sistema, secondo Parno, «non fornisce una grande garanzia».

L'impostazione di Pinocchio potrebbe venire usata anche per migliorare la privacy del sistema che raccoglie dati personali e li invia a un server centrale. I contatori elettrici intelligenti, per esempio, raccolgono dati abbastanza dettagliati da rivelare quali dispositivi esistono in una data casa e quante persone vi si trovano.

La bolletta di una famiglia viene calcolata inviando tutti questi dati al provider, ma potrebbe anche venire calcolata localmente, se il provider potesse controllare che qualcuno non abbia riprogrammato il dispositivo per ottenere uno sconto. «Il provider cloud», precisa Parno, «potrebbe richiedere al contatore di fare i conti, in modo da evitare una rilettura».

L'idea di utilizzare un sistema come Pinocchio era stata già proposta, ma le precedenti implementazioni richiedevano più tempo per controllare un risultato che per svolgere il lavoro. Anche con Pinocchio, alcune operazioni di controllo richiedono più lavoro di quanto non sia necessario per ripetere semplicemente i compiti originali, per cui, anche se funziona molto meglio dei prototipi precedenti, non è ancora pronto per una utilizzazione reale. ■

Tom Simonite è redattore di MIT Technology Review.