PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4247 di Mercoledì 30 maggio 2018

Finalmente possibile attivare sistemi di cifratura hardware a basso costo

Il regolamento generale europeo sulla protezione dei dati incoraggi in ogni modo l'adozione di sistemi di cifratura dei dati. Alcuni ostacoli oggi presenti sono stati superati da un recente sviluppo tecnologico.

Ormai nessuno dubita del fatto che i protocolli di cifratura a chiave pubblica siano i più efficienti ed efficaci disponibili. Tuttavia essi sono alquanto complicati nell'uso, perché sono normalmente sviluppati da software, assorbendo una grande quantità di risorse e rendendo difficile la loro applicazione in apparecchiature periferiche, come ad esempio sensori IoT.

Ecco perché è particolarmente attraente un nuovo sviluppo, che mette a disposizione degli apparati cifranti, in hardware, che assorbono una minima quantità di energia e operano con una velocità decisamente superiore a quella delle applicazioni software.

I ricercatori del Massachusetts Institute of Technology hanno sviluppato infatti un chip che può calcolare cifrature a chiave pubblica assorbendo soltanto la 400ª parte della energia elettrica che normalmente è necessaria per sviluppare la stessa applicazione cifrante in software. La velocità di elaborazione è 500 volte più veloce del più rapido software disponibile e quindi questo chip può trovare applicazione su larga scala, laddove i tempi tecnici di ritardo, introdotti dal software di cifratura, non sono compatibili con le esigenze operative.

Tipicamente un modulo cifrante può essere in grado di gestire numeri da 16 o perfino 32 bit. Per grandi masse di calcolo, il risultato di moltiplicazioni utilizzando numeri a 16 o 32 bit viene integrato utilizzando dei circuiti logici additivi.

Il nuovo modulo messo a punto dai ricercatori può gestire addirittura numeri da 256 bit, senza bisogno di circuiti aggiuntivi, che assorbono energia ed allungano i tempi di calcolo.

Viene così risolto un dilemma, davanti al quale si trova qualunque specialista di criptografia, che deve trovare un equilibrio tra la sicurezza dell'algoritmo crittografico e la rapidità di calcolo. Tutto ciò deve avvenire con un minimo assorbimento energetico e, almeno fino a oggi, un soddisfacente compromesso tra queste tre esigenze non era disponibile.

Ci auguriamo che questo nuovo chip di cifratura per algoritmi a chiave pubblica sia presto disponibile sul mercato, perché sarà così possibile proteggere in modo efficiente ed efficace i nostri preziosi dati personali, cui il regolamento generale europeo, entrato pienamente in vigore il 25 maggio 2018, presta grande attenzione.

Adalberto Biasiotti
