Il Futuro dell'Identità Digitale è a Torino

I ricercatori di LINKS lavorano sull'identità digitale di persone ed oggetti

Di Andrea Vesco, Head of Cybersecurity Fondazione LINKS

La sempre maggiore diffusione di servizi digitali fruibili in rete richiede la disponibilità di strumenti capaci di gestire e controllare in modo semplice ed efficace l'identità delle persone, nel massimo rispetto della loro privacy. Il concetto di *identità digitale* rappresenta una tematica che ha recentemente riscosso un grande interesse e su cui si sono concentrati notevoli sforzi ed investimenti, ad esempio per l'implementazione della Certificazione Verde COVID-19 e di altri sistemi analoghi.

L'**Identità Digitale** è l'insieme dei dati e delle informazioni, o attributi, che definiscono il Titolare e costituiscono la rappresentazione virtuale dell'identità reale utilizzabile durante interazioni elettroniche con persone o sistemi informatici).

Il gruppo di ricerca sulla Cybersecurity della Fondazione LINKS di Torino lavora da anni sul tema dell'identità digitale e presidia diverse tecnologie emergenti nell'ambito della sicurezza informatica. Le attività di ricerca si focalizzano su nuovi algoritmi e protocolli crittografici che permettono di gestire in modo sicuro e decentralizzato le credenziali digitali, ovvero le informazioni che l'utente utilizza per farsi riconoscere dai vari portali e sistemi informativi (l'esempio più noto di credenziali è rappresentato dalla coppia username e password).

Queste nuove soluzioni non richiedono la presenza di un'autorità centrale, ovvero un "*fornitore di identità*" incaricato di emettere le credenziali, e di terze parti incaricate della verifica di tali credenziali. Vengono così abilitati nuovi paradigmi in cui una specifica credenziale può essere gestita in piena libertà ed autonomia dal suo possessore, *democratizzando* così il concetto di identità digitale e garantendo un giusto livello di privacy a tutti gli utenti del sistema.

Una soluzione ideale di questo tipo deve anche permettere ad ogni utente di rivelare il minimo insieme di informazioni legate alla sua identità che sono necessarie per la sua identificazione e per aver accesso ad un certo bene o servizio (ad esempio il fatto di avere un'età superiore ai 18 anni, senza rivelare il dettaglio di luogo e data di nascita). In questo modo, l'utente non deve necessariamente rivelare informazioni strettamente personali e/o sensibili (come le numerose informazioni presenti sulla sua carta d'identità, non sempre rilevanti per un determinato scopo).

Questo approccio, che punta a conferire agli utenti la gestione della propria identità, è conosciuto con l'acronimo inglese *Self-Sovereign Identity* (SSI): esso rappresenta un modello per la gestione dell'identità digitale su Internet che è emerso di recente e che sta diventando una delle tendenze più importanti nell'ambito della ricerca e sviluppo europea e mondiale. Il modello SSI sfrutta il paradigma dell'identità decentralizzata mediante due tecnologie software principali: i *Decentralized Identifiers* (DIDs) e le *Verifiable Credentials* (VCs) le cui specifiche sono tema di dibattito presso il *World Wide Web Consortium* (W3C). Queste credenziali digitali vantano un'alta interoperabilità e portabilità, che le rendono adatte ad essere impiegate in diversi settori applicativi.

Il modello di identità SSI è da considerarsi la soluzione ad oggi disponibile più avanzata. Tuttavia la ricerca non si può fermare, e già si sta studiando come far fronte al suo limite più evidente: il fatto che queste credenziali fanno uso della crittografia classica, un domani potenzialmente vulnerabile a causa dell'avvento dei computer quantistici (*i.e.*, *Quantum-vulnerable*). Questo tipo di computer non rappresenta più solo una remota ipotesi teorica, ma è una concreta possibilità futura, dato che esistono già ad oggi dispositivi con una potenza di calcolo di diverse decine di bit quantistici (*i.e.*, circa 60 qubits).

Per questo motivo i ricercatori Cybersecurity della Fondazione LINKS stanno studiando le più promettenti soluzioni crittografiche robuste contro i futuri computer quantistici (*i.e.*, *Quantum-resistant*), adattandoli agli attuali schemi di credenziali digitali e proponendone evoluzioni più sicure delle versioni attuali.

Il gruppo di ricerca lavora inoltre all'estensione dei sistemi di credenziali per renderli adatti a gestire non solo l'identità digitale delle persone, ma anche delle cose. Viviamo infatti ormai in un mondo di oggetti connessi (ovvero l'*Internet delle Cose* – *Internet of Things*), nel quale robot, droni e veicoli a guida autonoma stanno diventando sempre più diffusi. Diventa quindi urgente poter assegnare identità univoche, scalabili, sicure e facilmente verificabili anche agli oggetti.

Su queste tematiche il gruppo di Cybersecurity della Fondazione LINKS collabora attivamente con diversi enti in ambito internazionale, tra i quali il Politecnico di Torino.