LA RICERCA Da Povo a Seattle, l'esperienza della ricercatrice che ha ideato il sistema che permette di confrontare dati criptati

I segreti che interessano a Microsoft

DANIELE BATTISTEL
d.battistel@ladige.it

Da Povo al quartier generale mondiale della Microsoft portando con sé i segreti (visto l'argomento è proprio il caso di dirlo) degli schemi di criptografia.
Comincerà nei prossimi giorni l'avventura americana di Mihaela Ion, giovane ricercatrice di origine romena che da quattro anni lavora a Create-net e che recentemente è stata selezionata dall'azienda fondata da Bill Gates per svolgere un periodo lavorativo presso la sede principale del gruppo, a Redmond (nei pressi di Seattle).
La Microsoft si è interessata a lei dopo aver avuto occasione di visionare il suo lavoro nel campo della sicurezza dei dati in rete.
In particolare Mihaela Ion, sotto la supervisione del ricercatore senior Giovanni Russolo, ha elaborato degli schemi di criptografia che permettono di effettuare delle operazioni di confronto dei dati senza visionarli completamente, bensì direttamente nella loro versione criptata. Così si elimina il pericolo che durante la trasmissione via web i dati personali possano essere visualizzati da terzi.
La collaborazione con la ricercatrice di Create-net è stata voluta proprio dall'azienda americana che, dopo aver visto il suo curriculum scientifico, l'ha invitata ad uno stage di tre mesi.
L'ambito in cui da anni Ion lavora assieme a Russello e al professor Bruno Crispo (associato del Dipartimento di informatica e scienze dell'informazione di Povo) è decisamente molto particolare. L'obiettivo ultimo degli loro sforzi è creare un sistema per trasmettere dati criptati e che, pur essendo virtualmente «a disposizione» di tutti, possono essere utilizzati solo da chi ha gli strumenti in grado di «intercettarli». Il problema su cui ci si è concentrati non è tanto la decrittazione quanto la ricerca di un sistema che sia in grado di estrarre da un archivio criptato un'informazione criptata. La Microsoft, decisamente interessata al sistema, fornirà a Ion la possibilità di testarlo e perfezionarlo.
Le possibili applicazioni concrete di questa nuova conquista rendono chiara, meglio di tante spiegazioni teoriche, la sua importanza. Si potrà, per esempio, utilizzare questo sistema in campo medico. Le aziende sanitarie, anziché dover mantenere costosi cervelloni di memoria, potranno lasciare le cartelle sanitarie dei pazienti su un contenitore «virtuale» permettendo al medico di accedervi in qualsiasi situazione in modo sicuro. Grazie al nuovo sistema la sua richiesta criptata sarà infatti «riconosciuta» dal contenitore che fornirà una e una sola cartella, senza intromissioni nella privacy.

Lo schema permetterà di abbattere i costi di cura e sicurezza delle informazioni sensibili

TUTTO EBBE INIZIO CON «ENIGMA»

I più antichi modelli di criptografia risalgono ai temi dei faraoni egiziani e al loro sistema di geroglifici, ma è nel ventesimo secolo con l'invenzione della macchina Enigma a rotori che la tecnica della scrittura in codici fa un decisivo passo in avanti. Essa fu alla base del dominio delle forze armate tedesche durante il primo periodo della seconda guerra mondiale. Soltanto dopo anni, e grazie agli sforzi di polacchi e inglesi, si riuscì a creare una macchina in gradi di decrittare i messaggi cifrati dando così importantissime informazioni agli alleati.
Da lì, con l'introduzione dei computer i sistemi di cifratura sono sempre più complessi e difficili da decodificare per chi non ha le chiavi.

Il team

Si chiama «Security group» e da un anno e mezzo lavora dentro Create Net per sviluppare un sistema in grado di poter trasmettere dati sicuri su internet pur attraverso molteplici «nodi». Ne fanno parte la ricercatrice Mihaela Ion, 28 anni, il ricercatore Giovanni Russello, 35 anni, e il professor Bruno Crispo del Disi.