

Sicurezza e peer-to-peer: tra anonimato e fiducia

Davide Cerri

Le applicazioni *peer-to-peer* (P2P) sono salite agli onori della cronaca alcuni anni fa con il “fenomeno Napster” e i suoi eredi (come ad esempio Gnutella), per cui vengono comunemente associate allo scambio di file musicali e simili tra utenti, con le conseguenti polemiche relative alla protezione del copyright. Al di là di questi utilizzi più o meno leciti, il peer-to-peer è comunque innanzitutto un *paradigma di comunicazione*, e come tale mantiene intatto il suo interesse tanto nel mondo della ricerca quanto in quello di applicazioni già oggi effettivamente utilizzate. Sul primo versante, è ad esempio di recentissima costituzione (giugno 2003) un gruppo di ricerca sul peer-to-peer all’interno dell’IRTF¹ (Internet Research Task Force, organizzazione gemella della più nota IETF). Nel secondo campo, architetture peer-to-peer (più o meno pure) si possono trovare ad esempio in piattaforme di instant messaging, marketplace, applicazioni di tipo collaborativo. La diffusione di applicazioni P2P è poi favorita dalla disponibilità di collegamenti a larga banda presso il grande pubblico, per cui qualunque utente di Internet può partecipare a comunità di questo tipo, senza dover passare per portali o server centralizzati.

P2P e sicurezza Lo sviluppo di sistemi peer-to-peer su larga scala pone tra le altre cose nuovi problemi dal punto di vista della sicurezza. I sistemi P2P, infatti, permettono collegamenti diretti tra utenti che in genere non si conoscono. Mentre quando si collega al sito di un’azienda o di un’istituzione nota l’utente sa con un discreto grado di sicurezza chi è il soggetto con cui ha instaurato il rapporto (quantomeno se è presente qualche forma di autenticazione), in una rete peer-to-peer è spesso impossibile ottenere un grado di fiducia comparabile, perché in genere l’utente non conosce il proprio interlocutore. La protezione della *privacy* (e quindi anche dell’*anonimato*) degli utenti su Internet è per altro un diritto fondamentale che deve essere protetto, per questioni di riservatezza personale e anche per garantire la libertà di espressione e la libera circolazione dell’informazione. Questo è stato tra l’altro puntualizzato lo scorso 28 maggio dal Comitato dei Ministri del Consiglio

¹<http://www.irtf.org/charters/p2prg.html>

d'Europa nella *Dichiarazione sulla libertà di comunicazione su Internet*², dove si afferma che “al fine di assicurare la protezione contro la sorveglianza in rete e di accrescere la libera espressione di informazioni e idee, gli stati membri dovrebbero rispettare la volontà degli utenti di Internet di non svelare la propria identità”.

È evidente, tuttavia, che le forme più forti di anonimato rendono problematica la creazione di un rapporto di *fiducia* tra i nodi. Inoltre, anche in casi in cui i nodi non sono strettamente anonimi, rimane il problema che, soprattutto in reti in cui si trovano migliaia di utenti, è sempre difficile per il singolo utente fidarsi di interlocutori di cui sa comunque poco o nulla, un po' come avviene ad una persona quando si trova in una città nuova in cui non conosce nessuno. Si vede dunque un potenziale contrasto tra due esigenze che hanno entrambe a che fare con la sicurezza: da un lato l'esigenza di proteggere la privacy degli utenti, e dall'altro la necessità di avere elementi in base ai quali decidere con quali altri utenti si vuole avere a che fare e con quali no.

Riservatezza e anonimato È indubbio che un grosso problema relativamente alle comunicazioni in rete è quello della privacy. Un problema dato dalla relativa semplicità con cui è possibile ottenere informazioni personali o addirittura tracciare il comportamento di un singolo utente, con il rischio che si possano dedurre dati sensibili come gli orientamenti politici, religiosi, sessuali, o le malattie da cui un individuo è affetto. Si pensi solo alle conclusioni che si potrebbero trarre su una persona conoscendo la lista dei libri che ha comprato o consultato negli ultimi mesi, o i file che ha richiesto a una community o ha messo in condivisione con gli altri.

Rendere anonimi gli utenti di una rete non è un problema semplice da risolvere, e purtroppo non è forse nemmeno molto sentito; vediamo brevemente se e come hanno affrontato questo punto critico alcuni noti sistemi peer-to-peer. *Napster*, per cominciare, non prendeva in considerazione il problema: tutti gli utenti comunicavano ad un server centrale quali erano i file che volevano condividere, e le ricerche avvenivano chiedendo direttamente al server centrale, che disponeva di tutte le informazioni; l'effettivo trasferimento del file era poi effettuato tramite connessione diretta tra i due peer interessati. In *Gnutella*³ un certo grado di anonimato è invece in parte garantito: le ricerche sono infatti effettuate in maniera sostanzialmente anonima, in quanto le “query” (richieste di risorse) vengono propagate in flooding (cioè “inondando” i nodi vicini) e non contengono l'indirizzo del mittente. La stessa cosa non avviene però per le risposte, che vengono retropropagate verso il nodo che aveva fatto la richiesta ma contengono l'indirizzo del nodo che possiede la risorsa, il quale quindi si “scopre” e perde l'anonimato. Quando poi il nodo richiedente decide di scaricare la risorsa da un certo nodo che la possiede apre con

²http://www.coe.int/T/E/Communication_and_Research/Press/News/2003/20030528_declaration.asp

³<http://gnutella.wego.com/>

lui una connessione diretta, perdendo quindi anche il suo anonimato. Il più noto e importante progetto peer-to-peer per quel che riguarda la condivisione anonima di risorse è *Freenet*⁴. Questo più che un sistema di file sharing (come Napster e Gnutella) è un sistema di pubblicazione contenuti, progettato per essere anonimo e resistente alla censura. In Freenet infatti le risorse non rimangono sul nodo originario, ma quando vengono richieste si propagano e si replicano all'interno della rete, in modo che non sia possibile stabilirne l'origine.

In generale, per proteggere l'anonimato si possono utilizzare diverse tecniche. La soluzione più semplice consiste nell'utilizzo di un proxy che faccia da intermediario tra i due interlocutori; in questo modo però si è spostato il problema dall'interlocutore al proxy, che conosce sia il mittente che il destinatario e verso il quale non c'è quindi nessuna garanzia di anonimato. Una soluzione possibile è allora aumentare il numero di intermediari, in modo che non ci sia un singolo proxy che vede entrambi gli estremi della comunicazione: in questo modo si potrebbe dire che la garanzia di anonimato è tanto più alta quanto maggiore è il numero degli intermediari. Un approccio di questo tipo è seguito nelle reti *MIX* (un esempio sono i remailer anonimi), dove il mittente di un messaggio decide di farlo passare per una catena di intermediari (i nodi *MIX*) e lo cifra "a cipolla" con le chiavi pubbliche degli intermediari stessi: in questo modo ogni nodo intermedio vede solo il nodo precedente e il nodo successivo nella catena, ma non può collegare mittente e destinatario. I nodi *MIX* compiono inoltre alcune operazioni che servono a confondere un eventuale osservatore, ad esempio inviando i messaggi in un ordine diverso rispetto a quello in cui li hanno ricevuti. Proprio l'idea di sfruttare la "confusione" è alla base di altri sistemi per l'anonimato. Nel caso del singolo proxy cui si accennava sopra, si potrebbe dire che paradossalmente l'unico ad essere veramente anonimo è il proxy stesso, in quanto l'eventuale traffico originato da esso si perde nella grande massa di quello da esso inoltrato, e dunque diventa indistinguibile. L'idea è allora quella di "confondersi tra la folla": facendo da intermediari per il traffico altrui vi si può facilmente nascondere il proprio, e quindi essere anonimi in quanto non è possibile dire se un messaggio proveniente da un certo nodo è stato effettivamente generato da quel nodo oppure da un altro. Un approccio di questo tipo è seguito da sistemi quali *Crowds* e *GNUnet*⁵: in questo caso si può dire che la garanzia di anonimato per un nodo è tanto maggiore quanto più il nodo stesso fa da intermediario per le comunicazioni tra altri nodi.

Reputazione e fiducia In un contesto completamente anonimo, il problema della fiducia appare irrisolvibile, in quanto l'utente non ha nessuna informazione su chi sia il suo interlocutore. Tutela dell'anonimato e distribuzione della fiducia possono quindi sembrare inconciliabili, ma il contrasto diviene molto più debole se dall'anonimato puro si passa

⁴<http://www.freenetproject.org/>

⁵<http://www.ovmj.org/GNUnet/>

a forme di *pseudonimato*. Con questo termine si intende un contesto in cui ad ogni utente è associato un identificativo (lo pseudonimo): tale identificativo non ha alcuna relazione con l'identità reale dell'utente, che rimane dunque sostanzialmente anonimo (in genere inoltre l'utente può in qualunque momento decidere di cambiare pseudonimo, oppure utilizzare diversi pseudonimi), tuttavia permette di collegare diverse azioni compiute dallo stesso utente, che in base al suo comportamento può quindi costruirsi una *reputazione*. Si può allora pensare di raccogliere in qualche modo le opinioni di utenti che hanno avuto rapporti con la persona o il servizio in questione, valutarle in base a una certa metrica, e poi decidere se fidarsi o no. Sistemi di reputazione sono presenti in diversi contesti, quali ad esempio il sito di aste eBay (per valutare l'affidabilità degli utenti), il motore di ricerca Google (per il ranking delle pagine), o la community Advogato⁶. Si tratta però di soluzioni di tipo centralizzato, e quindi non direttamente applicabili a contesti tendenzialmente privi di qualunque "autorità" come le reti peer-to-peer. In questo caso si intuisce che il problema è più difficile da risolvere, ed è al momento più che altro oggetto di ricerca.

La costruzione di un sistema peer-to-peer che tuteli la privacy degli utenti ma che fornisca meccanismi di distribuzione della fiducia è quindi allo stato attuale in larga parte ancora una sfida, ma se fosse vinta avrebbe probabilmente potenzialità enormi, permettendo agli utenti di sviluppare vari tipi di rapporti e transazioni in rete senza dover ogni volta rivelare la propria identità e tutte le varie informazioni connesse, e potendo contare su una certa probabilità che tutto vada a buon fine. Il che non è forse poi così diverso da quello che spesso avviene nel mondo reale.

⁶<http://www.advogato.org/>. Esiste un'analogia community italiana all'indirizzo <http://persone.softwarelibero.org/>.