Come può un computer fidarsi di un altro computer?

Author : Francesco Ermini

Date : 26 novembre 2018

Introduzione

Negli ultimi cinquant'anni gli algoritmi crittografici hanno garantito segretezza e integrità nella trasmissione dell'informazione. Tuttavia la crittografia non può garantire la veridicità sulla natura del dato. Chiariamo il concetto con un esempio: se io cifro il numero dei miei anni (dichiarando di averne 5) con la chiave pubblica del lettore questo potrà correttamente decifrare l'età che ho dichiarato di avere, ma non potrà mai sapere se ho detto la verità.

Invece se il lettore chiedesse la mia età all'ufficio anagrafe del comune in cui risiedo saprebbe con certezza quanti anni ho.

Nel mondo internet "classico", anche detto internet delle persone, un'informazione è veritiera se la fonte da cui proviene è autorevole. Una fonte è autorevole se la sua identità è garantita sia nel mondo analogico grazie a norme e controlli periodici sia in quello digitale tramite certification authority.

Nel mondo internet "delle cose" (IoT) questo schema non va più bene. Le fonti da cui proviene l'informazione sono troppe per essere tutte garantite sia 'online' che 'offline'. Si parla di decine di bilioni di dispositivi connessi nel prossimo futuro.

A questo punto la domanda che ci facciamo è:

Come posso stabilire se un'informazione è veritiera se non posso fidarmi della fonte da cui proviene essendo questa priva di garanzie?

L'intento dell'articolo sarà quello di rispondere a questa domanda illustrando cos'è una Network of Trust e quali sono le vulnerabilità di cui soffrono queste reti. In seguito verrà brevemente introdotta la subjective logic.

Che temperatura c'è adesso a Honolulu?

Per contestualizzare meglio il funzionamento di una TON (trust overlay network) introduciamo un esempio. Consideriamo un sistema di rilevamento della temperatura secondo il modello di internet ‘classico’. La misura è frutto di numerose certificazioni e adempimenti di leggi: tipicamente l’azienda che offre il servizio meteo ha contratti con un’altra azienda che gestisce i sensori ed entrambe le aziende devono essere accreditate dall'istituto metrologico dello Stato interessato. A livello globale gli istituti metrologici sono accreditati in modo gerarchico dall'istituto metrologico internazionale. Così un’azienda italiana accreditata potrà comprare il dato relativo alla temperatura in America da un’azienda americana, anch'essa a norma, e sapere che il dato ricevuto è veritiero.

Ora immaginiamo un sistema di rilevamento della temperatura globale nel mondo dell’internet delle cose. Ci saranno decine di migliaia di aziende che offriranno a pagamento (pay-per-data) il servizio di lettura della temperatura per una o più città nel mondo. Accreditare tutte queste aziende a livello globale è praticamente impossibile.

In assenza di un sistema di accreditamento, la misura di temperatura fornita da un’azienda sarà veritiera se l’azienda si comporta in modo onesto, falsa in caso contrario. Il problema è capire di quali aziende ci si può fidare e di quali no.

Un’azienda italiana necessita di sapere la temperatura che c’è ad Honolulu. L’azienda italiana dovrà scegliere una tra le mille aziende che gestiscono i sensori di temperatura ad Honolulu. L’azienda italiana non ha mai avuto rapporti con nessuna delle aziende di Honolulu per cui non sa se la misura che gli verrà fornita sarà veritiera. Per evitare di essere truffata l’azienda italiana chiama una ditta spagnola (di cui si fida) per sapere quali sono le aziende più serie di Honolulu. Per confermare quanto detto da quella spagnola, la società italiana chiama anche un’altra impresa.

Dopo aver confrontato i vari pareri l’azienda italiana seleziona, tra le tante di Honolulu, quella che ritiene più affidabile (e che costa meno fissata la qualità). Dopo aver ottenuto il dato sulla temperatura la società italiana potrà a sua volta giudicare la veridicità della misura e di conseguenza suggerire o meno la ditta di Honolulu ad altre imprese.

Questo semplice meccanismo, automatizzato per ogni nodo della rete e calcolato ad ogni transizione, è alla base di una network of trust.

Le insidie in una Network of Trust

In una network of trust la fiducia di un nodo viene calcolata a priori, basandosi sulla fiducia diretta/indiretta espressa dagli altri nodi della rete e modificata nel tempo valutando la positività delle transazioni fatte da/verso quel nodo.

Non esiste un ente terzo di garanzia, la fiducia viene costruita dagli stessi nodi che fanno parte della rete.

Così i nodi che frodano il sistema, detti nodi selfish in letteratura, vengono penalizzati fino ad

essere esclusi dalla rete, mentre quelli onesti vengono premiati garantendo così l’affidabilità delle fonti, quindi la veridicità dell'informazione.

Tutto questo in teoria. In pratica le insidie che si nascondono dietro una network of trust sono molte e verranno discusse in seguito.

Iniziamo considerando il caso di un singolo nodo selfish che agisce in autonomia. Questo tenderà a fornire una misura non corretta della temperatura per cui verrà valutato negativamente dagli altri nodi della rete, individuato ed evitato di conseguenza. Ma le cose non sono così semplici.

Uno degli attacchi più noti in una network of trust è il così detto Sybil Attack. Ogni nuovo nodo che entra a far parte della rete avrà assegnato una reputazione neutra di default. Ci sono casi in cui il frodatore elimina il nodo che ha una cattiva reputazione e ne crea uno nuovo. La reputazione neutra del nuovo nodo è migliore della reputazione cattiva di quello vecchio. Possiamo pensare che lo stesso nodo perda la cattiva reputazione che aveva accumulato e continui a frodare il sistema all'infinito.

Un altro problema si verifica quando nel calcolo numerico della reputazione si perdono informazioni per normalizzare il valore e diminuire la complessità computazionale (migliore performance). Questo avviene ad esempio nell'algoritmo Eigentrust dove l’indice di trust è calcolato come differenza tra le transizioni positive e quelle negative. Un nodo truffaldino che effettua un numero leggermente superiore di transizioni positive rispetto a quelle negative potrebbe apparire come onesto: un nodo che effettui 900 transizioni negative e 100 transizioni positive sarebbe considerato al pari di uno che effettua 10 transizioni positive e zero negative.

Ma il vero problema di una rete di trust nasce quando più nodi orchestrati da uno stesso frodatore si coalizzano per valutare positivamente un nodo selfish.

Questo tipo di attacco è molto difficile da individuare perché questi nodi si comportano in modo onesto ma la rete non sa che sono orchestrati da un unico frodatore. Infatti i nodi realmente onesti danno fiducia a questi perché, di fatto, si comportano rettamente, ma essendo sotto il controllo del frodatore questi nodi mentono e valutano positivamente il nodo selfish. Così per la proprietà transitiva quelli realmente onesti si fidano di quello selfish.

Vero && Vero… è un'opinione!

Nel corso dell'articolo ho parlato di fiducia da un punto di vista qualitativo. In verità una rete TON si basa su algoritmi che attribuiscono alla fiducia un valore quantitativo. Alcuni di questi algoritmi si basano su un tipo di logica probabilistica detta subjective logic.

Nella logica tradizionale una proposizione è vera oppure falsa. Inoltre le proposizioni possono essere combinate secondo le tabelle di verità: AND, OR, XOR...etc.

Nella subjective logic si parla di opinione. Un’opinione è una quadrupla (b,d,u,a) dove:

b è la "belief mass": un valore tra 0 e 1 che indica con quale probabilità la proposizione è vera;

d è la "disbelief mass": un valore tra 0 e 1 che indica con quale probabilità la proposizione è falsa;

u è la "uncertainty mass" : un valore tra 0 e 1 che indica il grado di incertezza dell'opinione;

a è la "prior probability"; un valore tra 0 e 1 che indica il grado di fiducia in un nodo prima di ogni interazione.

La subjective logic è molto usata nelle reti di trust perché permette di definire delle operazioni con cui è possibile combinare le opinioni. Ad esempio se A ha un'opinione di B e B ha un'opinione di C, allora A calcola la fiducia in C come un'operazione 'serie' tra le due opinioni. Allo stesso modo si potrà calcolare l'opinione di un nodo come un'operazione "parallela" tra tutte le opinioni espresse verso quel nodo.

Una volta definito come calcolare la fiducia non resta che implementare l'algoritmo distribuito sui nodi della rete o centralizzato verso un unico nodo logico (tipo SDN).

Conclusione

Nel mondo dell'internet delle cose risulta difficile, se non impossibile, poter autenticare e accreditare ogni fonte di informazione. I frodatori sono sempre in agguato e per garantire la veridicità dell'informazione è necessario trovare meccanismi diversi da quelli usati fino ad oggi. Una rete di fiducia è un sistema che permette ai nodi della rete di collaborare per garantire l'onestà dei nodi e la veridicità delle informazioni. La scelta o la progettazione di una rete di fiducia deve tenere in considerazione le vulnerabilità note.

Articolo a cura di **Francesco Ermini**