

Trust: concetti generali e teoria formale

Seminario

**“Protocolli e politiche di sicurezza:
modelli formali”**

a.a 2010/11

Laurea Magistrale in Sicurezza Informatica:
Infrastrutture ed Applicazioni

Università di Pisa

Marco Alamanni

Il concetto di *trust*

Trust - “to have belief or confidence in the honesty, goodness, skill or safety of a person, organization or thing.” - Cambridge Dictionary Online.

In italiano viene tradotto con il termine *fiducia*.

E' un concetto che ricorre in varie discipline quali economia, giurisprudenza, filosofia, psicologia, scienze sociali, oltre che in informatica (in particolare nella sicurezza informatica).

Il concetto di *trust*

Il concetto di *trust* è generalmente espresso in termini di una relazione binaria tra un soggetto (***trustor***) che si fida di un'altro soggetto, il fiduciario (***trustee***).

Può anche essere una relazione:

- ♦ *Uno-a-molti*, che si può applicare ad un gruppo di entità come fiduciario
- ♦ *Molti-a-molti*, come la fiducia reciproca tra i membri di un gruppo
- ♦ *Molti-a-uno*, tra diversi soggetti verso un'unico soggetto.

Il concetto di *trust*

Un rapporto di fiducia raramente è assoluto.

Ci sono vari livelli di fiducia che dipendono da qualità del fiduciario quali competenza, affidabilità, onestà, sincerità, sicurezza, competenza e tempestività in relazione alla sua capacità di eseguire un'azione specifica o fornire un servizio specifico all'interno di un determinato contesto

Spesso non è simmetrico: la fiducia di A in B di solito non è la stessa fiducia di B in A o è a senso unico (*non reciprocità*)

La fiducia è soggettiva: dato lo stesso fiduciario, avrò diversi livelli di fiducia da parte di soggetti diversi.

Classi di *trust*

Il *trust* spesso è legato a un obiettivo (*goal*) [**Castelfranchi – Falcone**]. Un obiettivo è ciò che il soggetto che si fida vuole conseguire tramite il fiduciario o le aspettative che ha su di lui/lei.

In base all'obiettivo e al tipo di azioni che il fiduciario può compiere possiamo classificarlo come:

- ♦ Access : acceso alle risorse
- ♦ Provision : *provider* di servizi
- ♦ Delegation : delega per decisioni
- ♦ Identity : identità, es **X.509** e **PGP**
- ♦ Context : hardware, infrastrutture ecc...

Access trust

Access trust: l'azione del fiduciario comporta l'accesso alle risorse del soggetto che si fida. Esempi: fornitore di assistenza al sistema informatico di un'azienda; dipendente dell'azienda; software scaricato da Internet ed installato...

A seconda del livello di fiducia che ripongo nel fiduciario posso quindi specificare e implementare le opportune politiche di controllo degli accessi e di assegnazione dei privilegi sulle risorse

Provision trust

L'obiettivo è ottenere un servizio dal fiduciario (*provider* o *fornitore*).

In questo caso, il cliente non solo ripone fiducia nell'affidabilità e nell'efficienza della fornitura del servizio in sé, ma si aspetta anche:

- ♦ che il fornitore si attenga al trattamento dei propri dati personali come disposto dalle leggi vigenti sulla *privacy*
- ♦ metta in atto tutte le misure di sicurezza previste dalla legge per evitare che i propri dati vengano sottratti da malintenzionati.

Context trust

Riguarda la fiducia dell'utente nei confronti delle risorse e dell'*infrastruttura* che usa (es. pc, server, rete locale...)

Trusted computing: tentativo di creare una piattaforma di calcolo “fidata” mediante un insieme di componenti hardware – software e l'uso della crittografia.

L'obiettivo è quello di migliorare alla base la sicurezza dei sistemi consentendo solo l'esecuzione di codice “fidato”

Sviluppato dal ***Trust Computing Group (TCG)***, promosso da Intel, AMD, Hp, Ibm, Microsoft e altri

Context trust

Critiche al *trusted computing*:

- ♦ Utile più che altro ai produttori per implementare meccanismi **DRM** (***Digital Rights Management***)
- ♦ Privacy degli utenti minacciata
- ♦ Mancanza di libertà di scelta del software che si vuole installare ed eseguire.
- ♦ Perché dovrei fidarmi dei membri del TCG...?

"A 'trusted' computer does not mean a computer that is trustworthy." – Bruce Schneier

Trust Management

In ambito informatico il concetto di trust ha assunto molta importanza soprattutto con lo sviluppo di Internet e delle sue applicazioni, in particolare quelle legate al *business* e alla finanza, come l'*e-commerce*, il *banking on-line*, le transazioni finanziarie ecc...

Una specifica formale di *trust* costituisce la base per la specifica e l'implementazione di politiche e protocolli di sicurezza, soprattutto per quanto riguarda i sistemi distribuiti.

Trust Management - 2

In generale, le entità coinvolte in una relazione di fiducia sono distribuite e possono non avere una conoscenza diretta l'una delle altre, per cui vi è la necessità di meccanismi che supportino l'instaurazione di relazioni di fiducia tra di esse (***trust management***).

La gestione del *trust* affidata alle applicazioni aggiunge altra complessità alle stesse ed implica mancanza di flessibilità nella creazione di nuove relazioni di fiducia.

Modelli di Trust Management

Un *trust management* separato dalle applicazioni offre una soluzione più scalabile e flessibile per un ambiente distribuito.

Due modelli di gestione principali:

- ♦ Basata sulla reputazione (conoscenza, diretta o indiretta, del fiduciario). (es. **Web of trust**, modello di trust di Ebay).
- ♦ Basata su certificati, rilasciati da terze parti fidate (**trusted third parties**), le cosiddette **Certification authorities**.

Web of trust

Modello di gestione decentralizzato e non gerarchico.

La fiducia è transitiva (ma fino ad un certo limite).

Esempio tipico: in **PGP** il legame identità-chiave pubblica viene considerato valido se convalidato da un certo numero di utenti.

L'utente A conosce B, si fida di lui e firma la sua chiave pubblica

B conosce C, ha verificato la sua identità e ha firmato la sua chiave

Invia ad A la chiave di C firmata. Dato che A si fida di B, accetta la chiave di C come valida.

Web of trust - 2

Qualsiasi entità può agire come una CA.

Ogni chiave deve avere un grado di fiducia associato ad essa: unknown, untrusted, marginally trusted or completely trusted.

Una chiave è valida se:

- ◆ È firmata da un numero sufficiente di chiavi valide (ad es. da 1 completely trusted o da 3 marginally trusted)
- ◆ La catena di trust non è più lunga di n passi

Certification authorities

Rappresentano un modello di gestione di trust centralizzato e gerarchico.

Ogni entità deve avere un certificato firmato da un'autorità di certificazione (di cui tutti si fidano) per poter essere considerata fidata.

Il modello *Web of trust* può andar bene per lo scambio di email sicuro tra privati ma per applicazioni come l'e-commerce è necessaria un'infrastruttura per creare, distribuire e revocare certificati (ad es. **PKI** e **protocollo X.509**).

Teoria formale di trust in un sistema distribuito

Di seguito viene presentata una teoria formale di trust in ambiente distribuito basato sulla logica modale, proposto da **P. V. Rangan** [2].

Perchè non la logica classica?

- Perchè non può rappresentare i concetti di *possibilità* e *credenza*, fondamentali per definire una teoria formale di *trust*.
- Perchè presuppone una conoscenza globale del sistema da parte di tutti i soggetti, che invece è limitata al proprio stato e a quelli accessibili.

Richiami di logica classica

Una Logica è un formalismo che mi permette di rappresentare i fatti del mondo e che mi fornisce dei meccanismi per inferire nuova conoscenza.

Una Logica è costituita da:

- ♦ Un Sistema Formale per descrivere i fatti del mondo:
 - ♦ Sintassi (simboli atomici, regole sintattiche...)
 - ♦ Semantica (interpretazione)
- ♦ Una Teoria della dimostrazione: definisce le regole di inferenza con le quali siamo in grado di derivare nuove formule da quelle che conosciamo già.

Logica modale

La **logica modale** è un tipo di logica formale che estende la logica proposizionale classica per rappresentare elementi di modalità.

Nella logica modale abbiamo diversi modi in cui una formula può essere vera o falsa.

In particolare, una formula può essere:

- ♦ Vera/Falsa necessariamente, per forza in qualsiasi contesto.
- ♦ Vera/Falsa possibilmente, cioè in modo contingente ad una certa situazione.

Operatori modali

- ◆ \square necessità (è necessario che...)
- ◆ \diamond possibilità (è possibile che...)

I due operatori modali sono duali:

$$\diamond p \leftrightarrow \neg \square \neg p$$

$$\square p \leftrightarrow \neg \diamond \neg p$$

Esempi:

- è possibile che piova oggi, se e solo se non è necessario che non pioverà oggi;
- è necessario che piova oggi, se e solo se non è possibile che non pioverà oggi.

Semantica

Per gli operatori modali la semantica si definisce in termini di ***mondi possibili*** (**possible worlds semantics – S. Kripke, 1959**)

L'insieme dei mondi possibili è un insieme W (non vuoto) tale che, in ogni elemento di W , una formula può avere un diverso valore di verità a seconda del mondo.

Tra i mondi possibili esiste una ***relazione di accessibilità o possibilità*** R ($W \times W$): ad es. per $R(X, Y)$ si dice che il mondo Y sarà visibile dal mondo X (o che, per X , Y è un mondo possibile).

Semantica - 2

Semantica degli operatori modali:

- ◆ $\Box p$ è vero in X se e solo se p è vero in tutti i mondi:

$$v(\Box p, X) = T \leftrightarrow \forall Y \text{ in } W, v(p, Y) = T$$

- ◆ $\Diamond p$ è vero in X se e solo se p è vero in almeno un mondo:

$$v(\Diamond p, X) = T \leftrightarrow \exists Y \text{ in } W, v(p, Y) = T$$

Agenti e stati

Un sistema distribuito è modellato come un insieme di agenti, che si scambiano messaggi per comunicare tra loro.

Lo **stato** del sistema risulta dallo stato di tutti i suoi agenti.

Lo stato di un agente consiste nella storia di tutti i suoi messaggi, cioè la sequenza dei messaggi inviati o ricevuti dall'agente.

Un messaggio è costituito da una FBF, un mittente e un destinatario.

Il concetto di *belief*

Introduciamo il concetto di *belief* (**credenza** o **convinzione**) che è fondamentale per il nostro modello.

Definiamo l'operatore logico modale ***Bi*** la cui semantica è "l'agente *Ai* crede..."

La formula "*Bi p*" sta a significare che l'agente *Ai*, nonostante non possa dimostrare in assoluto la verità o la falsità di *p*, "crede", "si aspetta" sia vera.

beliefs (*s, i*) = l'insieme di *credenze* di *Ai* nello stato *si*

Struttura di Kripke

Kripke introdusse un modello formale per la semantica dei mondi possibili, la cosiddetta **struttura di Kripke** (*Kripke structure*).

Dato Φ come insieme delle proposizioni primitive, viene definita come una tupla (W, R, v) dove:

- ◆ W è un insieme di mondi o stati;
- ◆ v è una funzione che associa un valore di verità ad ogni proposizione di Φ per ogni stato w in W ;
- ◆ $R: W \times W$ è una relazione binaria di accessibilità tra mondi di W .

Teoria formale di trust in un sistema distribuito

Valgono le seguenti definizioni:

$$w \models p \leftrightarrow v(w,p) = 1$$

$$w \models (p \wedge q) \leftrightarrow w \models p \wedge w \models q$$

$$w \models \neg p \leftrightarrow \neg (w \models p)$$

$$w \models Bi p \leftrightarrow \forall w' \in W \mid R(w, w') \ w' \models p$$

L'ultima definizione, in particolare, afferma che un agente A_i “crede p ” se e solo se p è vera per ogni stato w' che A_i considera possibile quando si trova nello stato w .

Teoria formale di trust in un sistema distribuito

Un agente A_i acquisisce *credenze* nuove attraverso lo scambio di messaggi con altri agenti.

In modo informale, possiamo dire che se riceve una FBF p da A_j , aggiunge la *credenza* $B_i B_j p$ al proprio *insieme di credenze beliefs* (s,i) se e solo se $B_j p$ non è in contraddizione con le *credenze* acquisite in precedenza dai messaggi ricevuti da A_j .

La relazione di accessibilità R gode delle seguenti proprietà:

- Transitività:
 $\forall s,t,u ((s,t) \in R \wedge (t,u) \in R) \rightarrow (s,u) \in R$
- Proprietà euclidea:
 $\forall s,t,u ((s,t) \in R \wedge (s,u) \in R) \rightarrow (t,u) \in R$
- Proprietà seriale:
 $\forall s \exists t | (s,t) \in R$

Schema assiomatico

Possiamo ora definire uno schema assiomatico che ci fornirà un sistema formale completo e “sound” per la nostra logica:

A1. Tutte le istanze di sostituzione di tautologie proposizionali.

A2. $\Box p \wedge \Box (p \Rightarrow q) \Rightarrow \Box q$

A3. $\Box p \Rightarrow \Box \Box p$ (transitività)

A4. $\neg \Box p \Rightarrow \Box \neg \Box p$ (proprietà euclidea)

A5. $\neg \Box (\text{false})$ (serialità)

Regole di inferenza

Aggiungiamo le seguenti regole di inferenza:

$$\mathbf{R1.} \quad \frac{p, p \Rightarrow q}{q} \quad (\text{modus ponens})$$

$$\mathbf{R2.} \quad \frac{p}{\forall i p} \quad (\text{generalization})$$

Conclusioni

Abbiamo così formulato una base assiomatica per il nostro modello formale di *trust*.

Gli agenti acquisiscono nuove *credenze* o invalidano quelle già acquisite scambiandosi messaggi e applicando alle FBF le regole di inferenza, nel rispetto dei *vincoli* imposti dagli assiomi

Un modello formale analogo, sempre basato sulla logica modale, è usato in AI per rappresentare la *conoscenza* e la *credenza* e per progettare agenti software.

Conclusioni

Potremmo anche estendere il modello aggiungendo altri assiomi alla teoria che non la invalidino, cioè che siano soddisfacibili in essa.

Ad esempio potremmo imporre nuovi *vincoli* alle *relazioni di possibilità* nella struttura di Kripke.

Il modello ci fornisce quindi una specifica formale astratta di *trust* su cui basarsi per specificare protocolli di sicurezza.

Riferimenti

- [1] T. Grandison, M. Sloman, **A Survey of Trust in Internet Applications**
<http://pubs.doc.ic.ac.uk/TrustSurvey/>
- [2] P. V. Rangan, **An axiomatic basis of trust in distributed systems**, Proceedings of the 1988 IEEE conference on Security and Privacy
- [3] M. Dezani, **Introduzione alla Logica Modale**
www.educ.di.unito.it/~dezani/SEM/LUCIDI/Logica%20Modale.pdf

GRAZIE!