Preferenze privacy degli utenti

Parte IV

Indice

Capitolo 1

Introduzione

Privacy dell'identità degli utenti

Gli utenti preferiscono restare anonimi o comunque non condividere troppe informazioni quando operano nel cloud. Alcune situe:

- **Tecniche di comunicazione anonima**
- **Privacy in location-based services** (protezione della location quando sensibile)
- **Attribute-based control access:** è un problema lato server, non ci si basa più su chi un tente sia (l'identità) ma sugli attributi che ha (certificati che l'utente presenta)
- **Supporto alle preferenze privacy degli utenti** (problema lato utente)

Gli utenti potrebbero voler specificare le proprie scelte in termini di politiche del trattamento dei dati

- l'utente decide quali informazioni inserire quando utilizza server esterni (es. Facebook)
- quando vengono rilascite informazioni nelle interazioni digitali (controllo dle rilascio dei dati)

due aspetti della protezione:

- **rilascio diretto:** regola quando e perchè un utente rilascia informazioni (es. sto comprando qualcosa)
- **uso secondario:** regola l'uso e la profilazione dei dati da terze parti

1.1 Rilascio diretto

Definizione di meccanismi di **attribute-based access control** quindi di dipedenza dell'accesso rispetto alle proprietà che un utente ha. Quello che gli utenti possono fare dipende dagli attributi che possiedono, verificati dai **certificati**

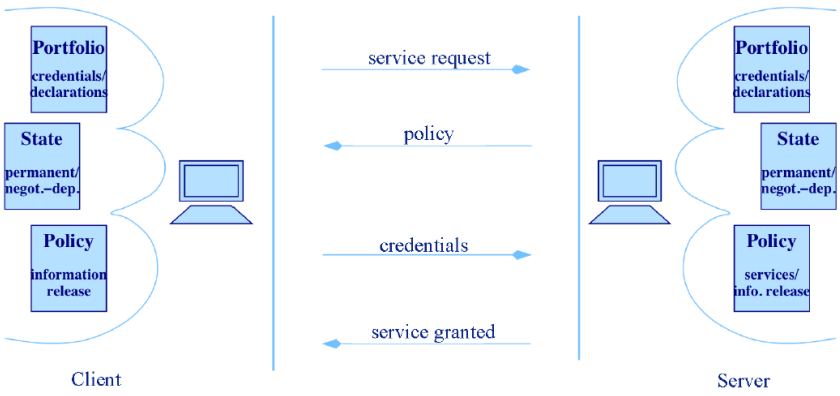
L'access control non risponde più si o no, ma risponde con i requisiti che il richiedente deve soddisfare per avere l'accesso. Non solo i server vanno protetti ma anche gli utenti, per questo vanno introdotte *forme di negoziazione*

Varie proposte tra cui:

- credential/attribute policy specifications
- policy evaluation con informazioni parziali
- policy confidentiality support (anche la politica stessa potrebbe essere confidenziale)
- policy communication and dialog (come comunichiamo la politica)
- strategie di negoziazione e trust management (richieste e dimostrazioni continue dalle due parti)
- valutazione di terminazione, correttezza, nessuna informzione impropria nella negoziazione

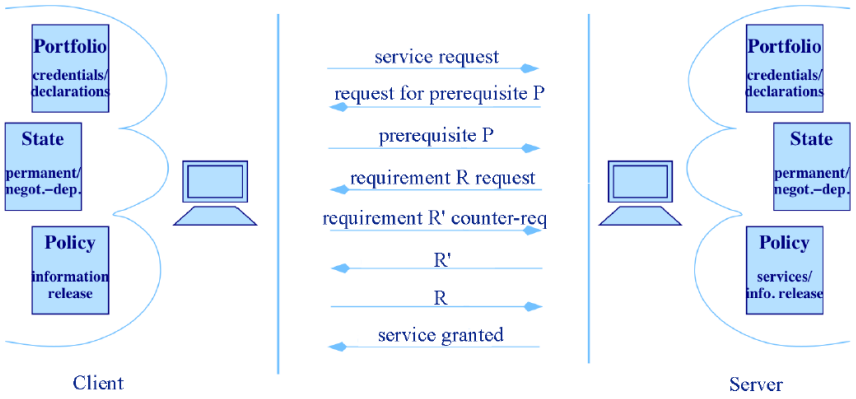
tipicamente vengono usati linguaggi basati sul paradigma logico

1.2 Controllo di acesso interattivo



Il client è colui che richiede il servzio, ha con se il suo **portoflio** (credenziali e proprietà), lo **stato** (stato di informazioni che vuole mantenere) la **politica**, lo stesso vale per i server che è colui che offre il servizio. La policy del server

sta ad indicare ciò che il client deve dimstrare, tramite i certificati, per poter accedere al servzio.
Negozziazione multi-step implica *Trust management* → stabilire fiducia tra le due parti.



Interazione a due step:

per essere gentili con l'utente separiamo i prerequsiti per l'accesso (necessari ma non sufficenti) e il requisito vero e proprio con eventuale controrichiesta da parte dell'utente.

Esistenti/emegenti tecnologie di supporto a ABAC

- U-Prove/Idemix: fornisce avanzate tecnologie di gestione dei certificati (i certificati odierni ti permettono di estrapolare dal certificato l'informazione senza fornire tutto il certificato).
- XACML: standard di oggi per l'interoperabilità delle politiche di controllo degi accessi

Le specifiche di controllo degli accessi non sempre fittano bene con il problema lato utente: Di positivo hanno che sono espressive,potenti e permettono all'utente di di specificare se determinate informazioni possono o non possono essere rilasciate. Di contro non permettono agli uenti di esprimere che preferirebbero rilasciare determinate informazioni piuttosto che altre, nel contesto in cui ne sia data la possibilità.

- **Context-based preferences** (lascio la carta solo quando devo pagare)
- **Forbidden disclosures** (non vogliono che diverse personalità social siano linkate)
- **Associazioi sensibili**

- **Limited disclosure**
- **Instance-based preferences**
- **History-based peferences** (magari ho già rilasciato qualcosa in passato)
- **Proof-based preferences**
- **Non-linkability preferences**