Un sistema per il controllo dell'accesso a Web Service: linguaggio, modello e architettura

Claudio Agostino Ardagna (matricola 580837)

Relatore: Pierangela Samarati **Correlatore:** Ernesto Damiani

La grande diffusione di Internet come mezzo di accesso alle informazioni rende sempre più pressante il bisogno, per organizzazioni e aziende sia pubbliche sia private, di garantire accesso via rete ai servizi da loro forniti o gestiti. Questa esigenza ha portato alla nascita e alla rapida diffusione dei Web Service, componenti software accessibili attraverso i normali protocolli in uso su Internet. Il modello a Web Service non si pone in concorrenza con le tradizionali architetture a componenti (CORBA, COM+, EJB) ma le affianca, permettendo di esporre componenti già esistenti verso nuovi client su architetture eterogenee. La forza del modello dei Web Service è di utilizzare un insieme base di protocolli disponibili ovunque, permettendo l'interoperabilità tra piattaforme molto diverse e mantenendo comunque la possibilità di utilizzare protocolli più avanzati e specializzati per effettuare compiti specifici. Gli standard alla base del modello a Web Service sono quattro: XML (eXtensible Markup Language), SOAP (Simple Object Access Protocol), WSDL (Web Services Description Language) e UDDI (Universal Discovery, Description ed Integration).

Il modello a Web Service è ancora molto giovane, quindi molti punti importanti presenti nelle architetture più diffuse sono ancora in attesa di una definizione e/o standardizzazione; ne sono un esempio la gestione della sicurezza, dell'autenticazione, dell'accesso, delle transazioni, dell'interazione fra più componenti.

Obiettivo del lavoro di tesi (realizzata in collaborazione con Marco Lupo Stanghellini) è il progetto e lo sviluppo di un sistema per il controllo dell'accesso a servizi che devono essere disponibili in modo selettivo tramite Web Service. Il lavoro propone una revisione al linguaggio WS-Policy e sviluppa un'implementazione dell'architettura proposta in grado di soddisfare parte dei requisiti del linguaggio di specifica delle politiche d'accesso.

Questa tesi è centrata sullo studio dei requisiti e dei linguaggi di definizione delle politiche e sulla proposta di un linguaggio e di un'architettura per la realizzazione del meccanismo di controllo. Il progetto di tesi si è sviluppato in più fasi e i contributi possono essere riassunti come segue.

- *Analisi dei requisiti.* È stata fatta un'analisi dei diversi requisiti di protezione che possono dover essere imposti sui servizi. Si è reso necessario l'utilizzo di un modello di controllo degli accessi semplice, ma allo stesso tempo potente e in grado di fornire controlli a granularità fine. Fra le varie possibilità, è stato scelto il modello a politiche di accesso.

- *Comparazione dei linguaggi.* Definito il modello, sono stati analizzati i linguaggi di specifica delle politiche già esistenti. Fra questi sono stati studiati in particolar modo WS-Policy e XACML mettendone in risalto peculiarità e differenze.

- *Studio e proposta di un linguaggio per la specifica delle politiche* Per il lavoro di tesi, è stato scelto il linguaggio WS-Policy che definisce una grammatica flessibile ed estendibile (fissando la sintassi e la semantica di ogni elemento) per rappresentare politiche di accesso più o meno complesse. WS-Policy si appoggia sulle specifiche WS-Security per la definizione degli elementi di sicurezza da inserire, in modo formale, all'interno dei messaggi SOAP. Le funzioni di WS-Security per la codifica, per la protezione delle informazioni e per la gestione delle firme digitali utilizzano i relativi standard XML; in questo modo, WS-Security può essere implementato anche su protocolli di trasporto molto semplici e sprovvisti di funzioni di crittografia senza perdere nessuna funzione di sicurezza.

  Il linguaggio WS-Policy definito da Microsoft è tuttora in fase di allestimento e ha ancora una serie di specifiche ambigue, a volte in disaccordo fra loro; in molti casi le definizioni sono interpretabili in maniera diversa a seconda del punto di vista di chi le legge. Per questi motivi, si è reso necessario revisionare le specifiche in modo da produrne una versione rigorosa. Il lavoro di controllo e rielaborazione è stato svolto in stretto contatto con alcuni sviluppatori della Microsoft ed ha portato alla ridefinizione di alcuni attributi, all'inserimento di alcuni nuovi elementi e all'eliminazione di attributi/elementi superflui o ambigui. Si è giunti quindi alla definizione di un linguaggio che si presenta completo, non ambiguo, formale, semplice e immediato, caratteristiche che permettono di rappresentare qualsiasi regola si voglia imporre, specificare meccanismi di scelta nel caso di contraddizioni e di ridurre al minimo la possibilità di errori nella stesura delle politiche di accesso.

- *Proposta di architettura per l'enforcement.* Trattata nel dettaglio dalla tesi di Marco Lupo Stanghellini, è composta da tre moduli:

  - PAP (Policy Administration Point) è un repository di politiche. Le ricerche all'interno di tale repository sono ottimizzate per produrre risposte rapide, anche nel caso di richieste contemporanee;
  - PEP (Policy Evaluation Point) si occupa di effettuare l'enforcement fra le politiche e la chiamata del client ad esso inoltrata rispondendo in maniera affermativa se almeno una delle politiche è rispettata;

– PDP (Policy Decision Point) riceve dal servizio la richiesta proveniente dal client. Si occupa di calcolare la risposta definitiva da restituire al client aggregando le singole risposte dei PEP.

Il lavoro di tesi lascia spazio a sviluppi futuri e possibili evoluzioni dell'architettura proposta. Prima fra tutte è l'integrazione dell'architettura di enforcement con lo standard UDDI per la ricerca automatica di Web Service. Lavori futuri riguardano anche l'estensione del PEP verso nuove specifiche del WS-Policy e dell'architettura verso altri linguaggi di specifica delle politiche (XACML).