Usare Grouper per gestire l'autorizzazione di Moodle

Andrea BIANCINI, Maria Laura MANTOVANI, Marco MALAVOLTI
Consortium GARR, Roma

Abstract

In questo lavoro verrà presentata un'esperienza di integrazione di Moodle con un sistema di gestione delle autorizzazioni centralizzato (implementato con uno strumento chiamato Grouper). Lo scopo delle attività descritte, sarà quello di mostrare come l'introduzione di Grouper permetta di ottenere semplificazioni nella gestione amministrativa dei corsi erogati tramite la piattaforma di e-learning. Inoltre, verrà discusso come l'uso di questo strumento centrale renda possibile la gestione di corsi erogati su più università, delegando le responsabilità di gestione ai soggetti più appropriati senza preoccuparsi dell'ente cui appartengano, e quindi semplificando i processi operativi.

Keywords: Moodle, Grouper, autorizzazione, Federazione di identità

Introduzione

Negli ultimi anni tutte le comunità nell'ambito della ricerca e dell'istruzione sono state molto attive nel promuovere le federazioni di identità [Gaedke et al., 2005]. Grazie a queste federazioni è stato possibile semplificare e migliorare i processi di autenticazione e la gestione degli accessi anche in ambienti eterogenei e complessi tipici della ricerca. Fino ad ora le federazioni d'identità, specie quelle create nell'ambito dell'istruzione e della ricerca, hanno ricevuto i benefici maggiori nell'implementare processi di autenticazione delegata.

Per raggiungere questi risultati le federazioni d'identità esistenti, per esempio quelle basate su SAML [Cantor et al., 2005b; Cantor et al., 2005a] e implementate con Shibboleth [Morgan et al., 2004], sono risultate molto efficaci. Esse hanno permesso di raggiungere ottimi traguardi nell'implementare processi e meccanismi di gestione federata delle identità. Lo stesso livello di accordo reciproco e sviluppo non è tuttavia ancora stato raggiunto nel campo dell'autorizzazione.

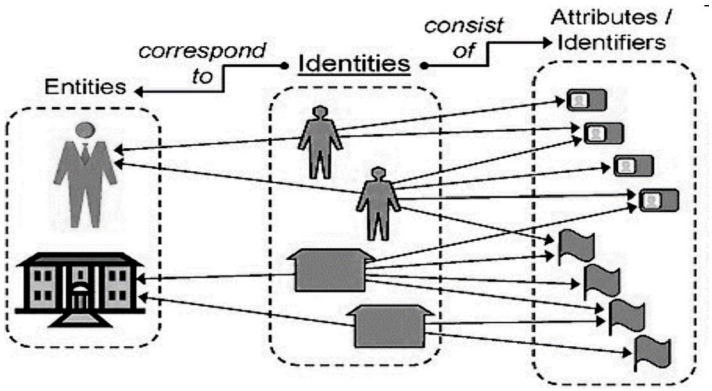


Figura 1 – I concetti chiave di un processo di autenticazione e autorizzazione

Insieme all'autenticazione, l'autorizzazione è un aspetto chiave dell'identity management. Nel seguito potremo rifarci alle seguenti definizioni per distinguere chiaramente autenticazione e autorizzazione:

- L'autenticazione è l'atto che, verificando la correttezza di uno (o più: dual factor) degli attributi di una certa identità, conferma la veridicità del corrispondente insieme di attributi, che insieme costituiscono l'identità (parziale) di una entità. Per esempio, superando la verifica della password (attributo), accetto anche gli altri attributi collegati ad essa (username, nome, ecc…), che insieme costituiscono l'identità e che mi rimandano alla corrispondente persona

reale (entità, ad es: l'utente di un'applicazione). Autenticare un utente, quindi, significa provare che egli è realmente chi dichiara di essere.

- L'autorizzazione, invece, è la funzione che specifica cosa una identità (non una entità) può fare in termini di quali informazioni può disporre e di quali funzionalità sono per essa abilitate quando usa una specifica applicazione. Più formalmente possiamo dire che "autorizzare" significa definire (per le identità) una politica di accesso alle risorse e alle funzionalità di un servizio. Nelle federazioni di identità è conveniente basare l'autorizzazione sugli attributi che costituiscono l'identità.

L'autorizzazione, anche in un ambiente di identità federate, attualmente rimane ancora un processo solitamente non federato, ossia finora è solitamente il gestore della singola risorsa che decide chi autorizzare.

In questo articolo descriveremo i primi risultati delle sperimentazioni eseguite nell'ambito della definizione di un processo di autorizzazione distribuito, in particolare: * un sistema centrale che può essere implementato come cuore del processo di autorizzazione; * il caso d'uso di integrazione di Moodle con questo sistema; * alcune conclusioni e sviluppi futuri.

Un sistema centrale di autorizzazione

Per implementare un processo di autorizzazione federato che incrementi i risultati ottenuti nel campo dell'autenticazione, proponiamo una soluzione che faccia leva sul concetto di Attribute Authority [Novakov, 2013]. La soluzione, da noi sperimentata e quindi implementata come pilota, utilizza un sistema centrale che può essere utilizzato per gestire in un unico punto tutti gli attributi autorizzativi in un contesto inter/intra federato. Questo componente centrale, che per semplicità chiamiamo Attribute Authority (AA), deve integrarsi con gli identity provider (IdP) e i service provider (SP) interessati al processo di autorizzazione ed esistenti nella federazione o nella interfederazione. La AA deve fornire degli attributi addizionali riguardanti l'utente, successivamente all'operazione di autenticazione. Esempi di attributi addizionali forniti dalla AA possono essere dati da: (i) il nome dei gruppi a cui l'utente fa parte; (ii) alcuni attributi addizionali che possono essere utilizzati per l'autorizzazione (ad esempio il ruolo che l'utente ricopre all'interno di ogni singolo gruppo a cui partecipa).

La AA deve inoltre esporre delle API che permettano l'interrogazione da parte di applicazioni al fine di ottenere informazioni di utilità, quali una lista di tutti i gruppi della AA o una lista di tutti gli utenti che partecipano a un determinato gruppo. Per standardizzare questo tipo di interrogazioni, sta emergendo un nuovo protocollo chiamato VOOT (Virtual Organization Orthogonal Technology) [Kremers, 2012], che potrebbe affermarsi come standard di riferimento per questi compiti. La AA utilizzata per gestire tutti gli aspetti autorizzativi, deve quindi essere in grado di fornire informazioni attraverso specifiche API che implementino il protocollo VOOT.

Lo strumento che è stato utilizzato per gestire il ciclo di vita degli attributi della AA è Grouper, sviluppato da Internet2. Grouper [Grouper, 2014] è un Sistema di gestione dei gruppi progettato specificatamente per soddisfare i bisogni delle università e delle istituzioni di ricerca. Il motivo principale per usare uno strumento come Grouper è che esso permette di delegare in modo controllato l'amministrazione dei gruppi e con esso collaborare, pur mantenendo il controllo, nei processi di autorizzazione e nella gestione degli attributi autorizzativi. Con Grouper è possibile definire gruppi, ruoli e permessi per molti scopi come popolare e amministrare comitati permanenti, team di ricerca ad-hoc, dipartimenti o classi. Definiti i gruppi, le applicazioni che si integrano con Grouper possono utilizzare le informazioni su gruppi, ruoli e permessi per effettuare decisioni di natura autorizzativa. Grouper è sviluppato in forma open-source e rilasciato con licenza Apache 2.0. Grouper è molto utilizzato per la gestione dell'autorizzazione in applicazioni distribuite ed è un progetto molto vitale, costantemente aggiornato ed esteso, tale da supportare nuovi casi d'uso e nuove funzionalità.

L'integrazione di Moodle

Lo schema autorizzativo descritto nei capitoli precedenti, è stato utilizzato per esternalizzare la definizione di corsi e partecipanti di Moodle. Moodle [Moodle, 2014] è una piattaforma in grado di

erogare dei corsi, disegnata per fornire a docenti, amministratori e studenti uno strumento unico da utilizzare per creare ambienti di apprendimento e studio personalizzati. Grazie all'integrazione qui descritta, è possibile esternalizzare la definizione dei corsi nel sistema centralizzato basato su Grouper. I corsi, così definiti, possono quindi essere gestiti da amministratori differenti, eventualmente appartenenti ad organizzazioni diverse.

Come visto Moodle è un'applicazione che implementa una piattaforma per erogare dei corsi. Tra i suoi principali utenti vi sono, come minimo, due ruoli: docente e studente. Considerando che i docenti e gli studenti possono cambiare, si rende necessario gestire un processo di autorizzazione specifico per ogni singolo corso. Per realizzare l'integrazione tra Moodle e Grouper, quindi, è possibile studiare un sistema in cui ogni corso sia definito e gestito come un gruppo in Grouper. Così facendo, i docenti e gli studenti verranno inseriti nel giusto corso se membri del giusto gruppo creato in Grouper. In base al ruolo che l'utente ha nel gruppo, egli verrà riconosciuto come docente o come studente del corso ad esso associato.

Moodle deve inoltre poter ottenere una lista complessiva di tutti i corsi da erogare e deve anche poter recuperare le informazioni sui partecipanti, in termini di studenti e docenti, di tutti i corsi. Queste informazioni non sono strettamente legate a un singolo utente che sta accedendo, ma sono dati ottenibili attraverso le interfacce VOOT.

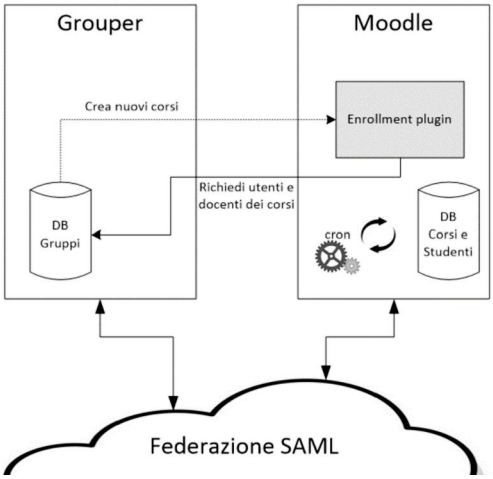


Figura 2 – L'integrazione di Moodle tramite l'enrollment plugin

L'integrazione con Grouper di Moodle è consistita nel creare un gruppo per ogni corso e, mediante l'impiego di un plugin specifico per Moodle, chiamato enrolment plugin, connettersi a interfacce esterne. Nel caso della nostra sperimentazione è stato appositamente sviluppato un nuovo enrolment plugin per Grouper che è in grado di interfacciarsi ad un server esterno e recuperare le informazioni sui gruppi tramite il protocollo VOOT [VOOT, 2014]) al fine di ottenere le informazioni sui corsi. Attraverso le interfacce VOOT è stato quindi possibile recuperare: (i) la lista dei gruppi in Grouper, che viene tradotta da Moodle in una lista di corsi da creare sulla piattaforma e (ii) i membri di ogni gruppo e i loro ruoli, questa informazione permette di determinare chi sono i docenti e gli studenti di ogni corso. Infine, un processo schedulato con cron sul server di Moodle tiene aggiornato il suo database rispetto ai gruppi/corsi definiti in Grouper.

Questa integrazione consente ad ogni utente di Moodle, dopo aver effettuato l'autenticazione federata, di vedere i materiali dei corsi a cui è iscritto come studente e di amministrare i corsi per i quali ha assunto il ruolo di docente. L'utilizzo dell'enrolment plugin consente di creare automaticamente nuovi corsi all'interno di Moodle, definendoli sotto forma di gruppi in Grouper. Le informazioni di accesso, per l'utente, vengono verificate ad ogni operazione di login, per evitare che ad uno studente o a un docente venga offerto un accesso cui non avrebbe diritto. Ad autenticazione avvenuta, quindi, gli attributi relativi ai gruppi di appartenenza degli utenti sono recuperati dalla AA e i diritti di accesso ai

corsi vengono aggiornate conseguentemente. Per realizzare questa integrazione, la componente SP del wiki, dopo aver interagito con l'IdP per autenticare l'utente, contatterà la Attribute Authority. Tale componente, collegandosi a Grouper, recupera le informazioni sul gruppo di appartenenza dell'utente e le trasmette a Moodle in modo che possa restringere l'accesso ai suoi contenuti in base al ruolo da lui ricoperto.

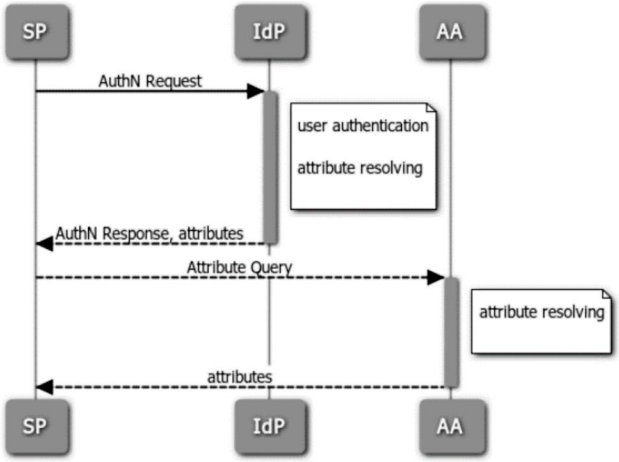


Figura 3 – L'integrazione di Moodle al login, tramite il meccanismo della AA

Conclusioni

L'introduzione di un sistema centralizzato per gestire l'autorizzazione degli utenti in ambiente federato ha permesso di disaccoppiare la gestione degli attributi autorizzativi sia dalla gestione dell'IdP che dalla gestione dell'SP e quindi di migliorare la distribuzione delle responsabilità nella gestione delle informazioni sugli utenti federati.

L'integrazione in un sistema autorizzativo centrale di Moodle, ci ha permesso di identificare alcuni elementi chiave di questo modello. I principali flussi di scambi informativi (online ed offline) sono stati identificati e il pilota realizzato ci ha permesso di apprezzare i vantaggi di utilizzare protocolli e interfacce standard nelle integrazioni tra i sistemi. Inoltre, usando uno strumento autorizzativo, esterno sia agli SP che agli IdP, come Grouper, è stato possibile implementare in maniera semplice meccanismi di delega granulare nella gestione degli attributi autorizzativi.

Riferimenti bibliografici

Cantor, S., Hirsch, F., Kemp, J., Philpott, R., and Maler, E. (2005a). *Bindings for the oasis security assertion markup language (saml) v2.0. Technical report.*

Cantor, S., Kemp, J., Philpott, R., and Maler, E. (2005b). *Assertions and protocols for the oasis security assertion markup language (saml) v2.0. Technical report.*

Gaedke, M., Meinecke, J., and Nussbaumer, M. (2005). *A modeling approach to federated identity and access management* in Special Interest Tracks and Posters of the 14th International Conference on World Wide Web, WWW '05, pages 1156–1157, New York, NY, USA. ACM.

Grouper (2014). http://www.internet2.edu/productsservices/trust-identity-middleware/grouper/.

Kremers, M. (2012). *Supporting virtual organisations using voot* in Internet2 Member Meeting, Fall 2012, Philadelphia, PA, USA. Internet2.

Moodle (2014). https://moodle.org/.

Morgan, R. L., Cantor, S., Carmody, S., Hoehn, W., and Klingenstein, K. (2004). *Federated security: The shibboleth approach* EDUCAUSE Quarterly, 27(4):12–17.

Novakov, I. (2013). *Standalone saml attribute authority with shibboleth* in CESNET Technical Report 5/2013, Prague, Czech Republic. CESNET.

VOOT (2014). https://github.com/andreassolberg/voot/wiki/Specifications.