1 Introduction to OpenID

La gestione dell'identità è emersa come uno dei campi più importanti della tecnologia dell'informazione, soprattutto nella sicurezza dell'informazione. La gestione dell'identità è un meccanismo primario per il controllo degli accessi. Ogni utente che deve accedere a un conto bancario, siti web, eCommerce o una risorsa dell'azienda ha bisogno di un'identità per i controlli di accesso appropriati.

Ci sono molti modi per creare e gestire le identità digitali. In genere, le identità vengono gestite a livello di sistema operativo o a livello di applicazione anche se esistono altri luoghi per gestire le identità. Nella gestione a livello di sistema operativo tre sono gli ambienti più comunemente utilizzati: Unix/Linux, Microsoft Windows, and Mainframe.

- In UNIX/Linux, la gestione dell'identità viene fatta in diversi modi: **LDAP**, **NIS**, **RADIUS**, **Kerberos**, e altri meccanismi.
- Nel mondo Microsoft, **Active Directory (AD)** è il meccanismo più utilizzato.
- Ci sono molti meccanismi per la gestione dell'identità nei sistemi mainframe come ad esempio **RACF** (Resource Access Control Facility).

Vediamo le definizioni di questi meccanismi e protocolli:

- **LDAP**, Lightweight Directory Access Protocol, è un protocollo standard per l'interrogazione e la modifica dei servizi di directory.
- **NIS - Network Information Service** (originariamente chiamato Yellow Pages o YP) è un protocollo per servizi di directory client-server per la distribuzione dei dati di configurazione di sistema, come utenti e nomi host, tra computer su una rete.
- **Servizio di directory** è un programma o un insieme di programmi che provvedono ad organizzare e memorizzare informazioni su reti di computer e su risorse condivise disponibili tramite la rete. Il servizio di directory fornisce anche un controllo degli accessi sull'utilizzo delle risorse condivise in modo da favorire il lavoro dell'amministratore di sistema. I servizi di directory forniscono uno strato di astrazione tra le risorse e gli utenti.
- **RADIUS** (Remote Authentication Dial-In User Service) è un protocollo AAA (Authentication, Authorization, Accounting) utilizzato in applicazioni di accesso alle reti o di mobilità IP. RADIUS è attualmente lo standard de-facto per l'autenticazione remota, prevalendo sia nei sistemi nuovi che in quelli già esistenti.
- **Active Directory** è un insieme di servizi di rete meglio noti come directory service adottati dai sistemi operativi Microsoft a partire da Windows 2000 Server.
- **RACF** (Resource Access Control Facility) è un prodotto per la gestione della sicurezza creato dalla IBM per i sistemi operativi dei mainframe.

Oltre alle soluzioni basate sui sistemi operativi per la gestione dell'identità, un numero di prodotti commerciali e open source sono disponibili anche per questo scopo. I prodotti forniscono strutture per gestire l'identità degli utenti su più piattaforme e servizi, come Single Sign On (SSO), Cross Company Authentication (CCA), etc. Aziende come RSA, Novell, Sun e gli altri forniscono prodotti commerciali per la gestione identità sofisticati più piattaforme.

In genere questi sistemi funzionano molto bene in un ambiente chiuso dove tutte le applicazioni e sistemi sono gestiti da un'unica società (sono centralizzati). Con la popolarità dei sistemi basati sul web, gli utenti comuni hanno account su diversi siti web e questo è dove inizia il problema. Un utente deve ora creare identità per tutti i siti web e ricordare nome utente e passwords. Ovviamente, ciò ha creato alcune questioni non solo per gli utenti, ma anche visto da prospettive di sicurezza. Il problema più comune dell'utente che ha diversi account su diversi siti web è:

come gestire le molte identità in molti siti web con i quali l'utente deve interagire ?

OpenID è un protocollo aperto che permette ad una persona di utilizzare un URL come identità e utilizzare la stessa identità (URL) in più siti web che supportano OpenID. Applicazioni Web che supportano OpenID possono utilizzare l'URL di identità per l'autenticazione, autorizzazione e altri scopi. È un concetto relativamente nuovo che mette il controllo dell'identità nelle mani del suo proprietario, l'utente finale. Il proprietario dell'identità può decidere, e ha il controllo, su quale informazione dovrebbe essere presentata ad un'applicazione o sito web per scopi di autenticazione. Tra le altre cose, OpenID permette di:

- Effettuare il login alle applicazioni web senza inserire nome utente e password
- Abilitare i siti web a richiedere informazioni dall'utente, e l'utente a scegliere con quale card (con quale informazione) presentarsi presso il sito durante il processo di autenticazione / autorizzazione.
- La scelta delle "card" dipende sia dalla necessità del sito per le informazioni necessarie sia dal livello di importanza dei dati. Ad esempio per i conti bancari l'utente presenterà una card con più informazioni.
- Implementare un'alternativa a SSO per applicazioni multiple all'interno della stessa società.
- Implementare un meccanismo alternativo a CCA per l'autenticazione cross-company.
- Costi minori nell'implementazione e gestione.