2 Authentication and Authorization

Per stabilire l'identità di qualcuno viene utilizzata l'**autenticazione** e l'**autorizzazione** viene utilizzata per concedere o negare l'accesso a una risorsa dopo l'autenticazione. Tradizionalmente, nelle applicazioni web-based, autenticazione e autorizzazione sono basate molto sul sistema.

Autenticazione e autorizzazione si stanno comunque muovendo verso una logica basta sull'utente, verso metodi **user-centric**. Gli obiettivi dei metodi di autenticazione e autorizzazione basati sull'utente sono:

- Dare il controllo all'utente dei token di protezione che vengono inviati a un sito web per l'autenticazione e autorizzazione.
- Consentire ai siti web di richiedere i token o ulteriori parametri in base al livello del rischio di informazioni a cui si accede.
- Consente ai provider di identità (identity provider) di rilasciare le identità digitali anziché username e password. Le identità digitali possono contenere diversi set di token a seconda delle esigenze e delle circostanze.
- Semplificare il processo di autenticazione per gli utenti finali.

Per soddisfare questi obiettivi, sono stati sviluppati diversi tipi di sistemi. OpenID è uno dei leader nell'area open source.

2.1 What is An Identity?

Non è una questione nuova: è stata lì per secoli, molto prima che i computer venissero inventati. L'identità è qualcosa che viene utilizzata per distinguere qualcosa o qualcuno da altri. Se pensate sull'identità degli esseri umani, può essere il nome di una persona? Probabilmente no, perché da qualche parte in questo mondo, ci potrebbero essere molte altre persone con il vostro stesso nome. Può essere il social security number, il colore degli occhi, la lingua che parla una persona, il luogo che vivete o qualcos'altro?

Nella maggior parte dei casi, l'identità è una combinazione di fattori sopra menzionati. Vedremo come l'identità può essere stabilita e gestita nel migliore dei modi..

2.2 Authentication and Authorization

L'origine di autenticazione viene dal greco e ha il concetto di autentico o genuino. L'autenticazione è l'atto o il processo che autentica qualcosa o qualcuno. Il significato di dizionario per l'autenticazione è: stabilire qualcosa (o qualcuno) come un'entità valida.

In termini di protezione del computer, l'**autenticazione** è un processo con il quale un'entità (un utente, un'applicazione, un dispositivo, ecc.) accerta un'altra entità per ciò che pretende di essere. Il metodo di autenticazione più comunemente utilizzato è il nome utente e una password.

L'**autorizzazione** è il processo che in genere viene dopo l'autenticazione e viene utilizzato per concedere o negare l'accesso a un risorsa (resource computing). Così una volta che una persona o un dispositivo è stato autenticato, l'autorizzazione abilita il controllo dell'accesso a una risorsa per solo coloro che hanno un bisogno legittimo per ottenere tale l'accesso.

Ad esempio, potrebbe essere necessario il distintivo del dipendente per stabilire l'identità e entrare nell'edificio della società (autenticazione). Tuttavia, solo ad alcuni dipendenti è consentito andare nella sala stampa (autorizzazione).

Si noti che l'autenticazione e autorizzazione vanno di passo-passo. L'autorizzazione a diverse risorse può essere concessa a seconda di una moltitudine di fattori, tra cui:

- La sensibilità e l'importanza della risorsa svolge un ruolo importante. Ad esempio, a solo poche persone può essere concesso l'accesso all'informazione finanziaria della società.
- Il metodo di autenticazione, il che significa che se una persona effettua l'autenticazione con nome utente/password più un dispositivo biometrico possa ricevere un più elevato livello di accesso rispetto a una persona che effettua l'autenticazione solo con username e password.
- Seconda il giorno e ora, è possibile ottenere diversi livelli di accesso, soprattutto in luoghi come le istituzioni finanziarie, ad esempio la borsa.
- La posizione dell'entità che deve accedere alla risorsa è anche un fattore importante. Ad esempio, una connessione proveniente da un paese ostile disporrà di pochissimi diritti di accesso per una risorsa. Alcune società finanziarie impongono agli utenti di fornire informazioni aggiuntive al momento dell'autorizzazione, se la connessione è provenienti da fuori agli Stati Uniti.

Autenticazione e autorizzazione sono vincolate ad una categoria di informazioni molto più ampia, la gestione dell'identità ("identity management"), che sta diventando una parte molto importante della strategia IT globale. OpenID semplifica diversi problemi in alcuni settori della gestione di identità.

2.3 Authentication Methods

L'autenticazione per sistemi di computer viene eseguita utilizzando metodi diversi. Dipendente da una situazione particolare, la sensibilità dei dati o del sistema, un metodo o una combinazione di metodi verrà utilizzata per l'autenticazione. In questa sezione vengono descritti alcuni dei metodi di autenticazione più comunemente utilizzati.

2.3.1 Password Authentication

L'autenticazione basata sull'uso della password è il metodo più comunemente utilizzo in tutti i sistemi e applicazioni. L'autenticazione tramite password è stata utilizzata per accedere a sistemi operativi, applicazioni client - server, applicazioni desktop, come pure applicazioni basate sul web. Per molta gente, quando si parla di autenticazione, username e password è la prima cosa che viene in mente. L'autenticazione basata su password ha completato il suo compito molto bene nel tempo.

Tuttavia, alcune questioni di sicurezza sono nate con l'autenticazione basata su password. La questione più comune è semplicemente il numero di combinazioni nome utente/password che una persona deve ricordare. Maggior parte degli utenti di computer hanno un account presso il loro posto di lavoro, la loro casa, la loro istituzione finanziaria, i fornitori di assicurazione, email account, etc. È diventato quasi impossibile da ricordare tutte queste password. Di conseguenza, gli utenti tipici saranno:

- Quelli che scriveranno le loro password da qualche parte
- Quelli che utilizzeranno la stessa password per tutti gli account.

Entrambe le situazioni non sono buone in prospettiva di sicurezza. Se si scrivono le password su un documento, se qualcuno si impossessa di tale documento la sicurezza verrebbe a mancare. D'altro canto, se si utilizza la stessa password per tutti gli account di posta, tutti questi account saranno compromessi se la password venisse scoperta. Poiché la stessa password è memorizzata in molti luoghi diversi, la probabilità di sua divulgazione aumenta con l'aumentare del numero di posti in cui è memorizzata.

Inoltre, nel corso del tempo, gli aggressori hanno trovato molti modi per ottenere le password e gli strumenti di password cracking sono diventati molto sofisticati.

Gli attacchi di phishing hanno rivelato carenze nell'utilizzo delle password come mezzo unico per l'autenticazione.

2.3.2 PIN Authentication

Il **PIN** o Personal Identification Number è una stringa di numeri o una combinazione di numeri e lettere. In genere un PIN è minore in caratteri rispetto a una password. I PIN vengono utilizzati in molti scenari come carte ATM, autenticazioni basate su sistemi telefonici, noti anche come Interactive Voice Response (IVR) e così via. I PIN vengono utilizzati anche in dispositivi palmari dove è impraticabile l'utilizzo delle password lunghe.

I PIN sono considerati un meccanismo di autenticazione debole e possano essere facilmente scoperti dalla ricerca esaustiva. L'uso di PIN è un meccanismo di autenticazione ragionevole, finché esso è utilizzato in combinazione con qualcosa che avete o qualcosa che si è, noto anche come l'autenticazione a due fattori.

2.3.3 One Time Password (OTP) Authentication

OTP viene utilizzata una sola volta per evitare problemi con le password compromesse. Esistono diversi modi per generare una OTP. L'impiego di token elettronici è uno di questi metodi.

Una volta generata la password tale password rimane in uso per un po' di tempo.

Questi sono generalmente piccoli dispositivi. Questi dispositivi generano stringhe di numeri casuali, su intervalli di tempo specificati oppure quando un utente preme un pulsante sul dispositivo stesso.

L'utente dovrebbe quindi utilizzare il numero casuale per l'autenticazione presso un sistema. In genere questo numero casuale viene utilizzato in combinazione con un nome utente o con una password, oppure con una carta.

2.3.4 Smart Card Authentication

Le smart card sono solitamente analizzate o inserita in un sistema per scopi di autenticazione. Smart card vengono usate sia per sicurezza fisica, nonché per la sicurezza IT. Queste carte sono in genere abbastanza piccole (dimensioni di una carta di credito) affinché le persone possono portarle comodamente.

Molte volte smart card vengono utilizzate in combinazione con un PIN. Smart card hanno dei nastri magnetici e/o chip incorporato che sono in grado di fare una serie di cose. Vi sono questioni di interoperabilità con smart card.

2.3.5 Biometric Authentication

Nei sistemi con l'autenticazione biometrica vengono usate, le impronte digitali, la scansione della retina, o qualche altro meccanismo di identificazione dove viene utilizzato il corpo. I sistemi biometrici non sono molto scalabili e hanno anche problemi di affidabilità oltre ad essere costosi da installare e gestire. Metodi biometrici, se non utilizzati correttamente, possono anche causare ulteriori rischi per la privacy.

In un tipico sistema biometrico, alla persona verrà richiesto di immettere un pin oltre alla autenticazione biometrica. Alcuni portatili inoltre utilizzino l'autenticazione biometrica senza immettere un pin tale che per l'utente non è necessario effettuare il login per il laptop.

2.3.6 Certificate Based Authentication

Digital certificates (noto anche come certificati **x.509**) vengono utilizzati anche come meccanismi di autenticazione in molti scenari. SSH (Secure Shell) è un esempio dove i certificati sono utilizzati spesso per lo scopo di autenticazione. Molte aziende utilizzano certificati come secondo fattore per l'accesso remoto, ad esempio ad una VPN. L'autenticazione basata su certificati è considerato molto sicuro se un infrastruttura adeguata per la gestione del certificato è disponibile.

Tuttavia, le infrastrutture possono essere avere costi proibitivi per molte aziende. I certificati digitali possono essere revocati quando un dipendente lascia una società o quando un certificato è perso o rubato. I certificati digitali hanno anche un meccanismo di scadenza. Qualsiasi sistema che si basa su certificati digitali per scopi di autenticazione è di solito in grado di controllare la validità del certificato, scadenza o revoca. I provider del certificato mantengono solitamente un elenco, denominato *Certification Revocation List* (CRL), che tiene traccia dei certificati revocati.

2.3.7 USB Devices

Alcuni dispositivi USB gestiscono le informazioni di autenticazione, come un certificato X.509. Dispositivi USB sono facili da gestire rispetto alla smart card e possano essere utilizzati anche per portare con sé altri dati. Un altro vantaggio è che lo stesso dispositivo USB possa essere utilizzato per accedere a più credenziali di accesso.

Come altre tecnologie, ci sono molti rischi connessi con i dispositivi USB. Il rischio maggiore è che la gente perde molto spesso tali dispositivi USB e utilizzando questi dispositivi per il trasferimento dei file da un luogo a altro, questo pone un rischio significativo per un certificato che può venire rubato o compromesso.

2.4 Weak and Strong Authentication

Persone diverse definiscono l'autenticazione forte e debole in modi diversi. Più comunemente è inteso che se solo la combinazioni di username e password vengono utilizzati per l'autenticazione su un sistema, allora l'autenticazione viene chiamata **autenticazione debole**. Tuttavia, se si utilizza una combinazione di diversi metodi di autenticazione in un sistema, si chiama un metodo di **autenticazione forte**. L'utilizzo di appena un nome utente e password è debole perché essa può essere compromessa abbastanza facilmente rispetto a qualsiasi metodo di autenticazione forte.

Per l'autenticazione forte, è possibile utilizzare più metodi o fattori. Ad esempio, token OTP è un fattore e la password è un altro fattore. Fattori sono divisi in tre grandi categorie:

- ***Something you know***
- ***Something you have***
- ***Something you are***

L'autenticazione forte usa una combinazione dei metodi appartenenti a queste categorie.

2.4.1 Autenticazione a due fattori

Quando si utilizzano due fattori in combinazione, il sistema di autenticazione viene chiamato **autenticazione a due fattori**. Ciascuno dei due fattori dovrebbe comportare un successo per autenticare la persona. Ad esempio, se si utilizza nome utente/password e token OTP, sia la username/password e stringa di token OTP dovrebbero corrispondere per avere successo nell'autenticazione. In questo caso anche se qualcuno scoprisse la password, non potrà effettuare il login a meno che non ottiene anche il dispositivo per la gestione delle token.

L'autenticazione a due fattori è consigliabile per le concessioni finanziarie, mediche e dati sensibili del cliente.

Si noti inoltre che utilizzando due volte lo stesso fattore non si ottiene l'autenticazione a due fattori. Ad esempio, utilizzando due password, anche se diverse, non rende l'autenticazione a due fattori. Per l'autenticazione a due fattori, si devono usare due fattori da due delle tre categorie elencate precedentemente in questo capitolo (cosa so,cosa possiedo o cosa sono).

2.4.2 Single Sign-On (SSO)

Anche per single sign-on SSO è difficile dare una definizione globalmente accettabile. Una definizione valida:

> **è un meccanismo secondo il quale è necessario effettuare il login una volta per ottenere l'accesso a più risorse.**

Così ad esempio, vi possono essere molte applicazioni nella rete aziendale. Tuttavia, quando si logga su un'applicazione e quindi si sposta su un altra , non è necessario autenticarsi nuovamente. Le credenziali sono consegnate a tutte le applicazioni che prendono parte in un sistema SSO e tutto questo avviene in background. A seconda del meccanismo di background utilizzato per SSO, alcuni dei meccanismi non sono considerati come veri SSO. In tali situazioni, viene anche chiamato "**accesso semplificato**" invece di un vero SSO.

SSO risolve una serie di problemi con username e password. Elimina la necessità di più username e password che sono difficili da ricordare. Con SSO, è possibile implementare migliori controlli per la difficoltà della password cosi che gli utenti devono scegliere una password difficile da trovare.

Tuttavia, SSO è come la chiave del castello, e se si perde, qualcuno può accedere a tutte le applicazioni e sistemi disponibili. È più prudente utilizzare SSO con l'autenticazione a due fattori in modo tale che anche se si perde una chiave non si può accedere a tutte le stanze del castello, cosi il rischio associato al sistema SSO è ridotto.

Molti sistemi sono sviluppati per SSO da diverse società. Kerberos è un sistema di tre parti che funziona sulla base di credenziali o biglietti. Inizialmente quando un utente accede al sistema, all'utente è concesso un biglietto. Quando lo stesso utente ha bisogno di accedere a un'altra risorsa della rete, un altro biglietto viene generato utilizzando il biglietto esistente.

In genere SSO viene utilizzato all'interno di una società e diventa inutile quando è necessaria l'autenticazione attraverso diverse società. Questo è perché un utente potrebbe avere uno username e password degli account di una società e un'altra serie di username e password per un'altra società. OpenID può essere utilizzato anche per SSO.

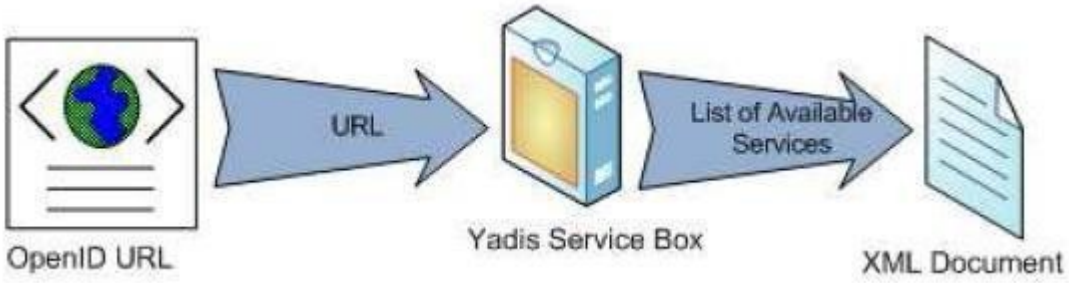
2.5 New Authentication Mechanisms - Yadis

Yadis fornisce un meccanismo per scoprire i servizi disponibili in un determinato URL.OpenID. È un semplice protocollo basato su XML e consente a un consumer di scoprire l'autenticazione nonché altri servizi forniti da un URL di identità.

Dato un URL di identità e nessun altra informazione, come facciamo a sappere quale protocollo deve essere utilizzato per autenticare l'utente? Yadis è un sistema di scoperta del servizio che consente al consumer (il Relayin Party) determinare automaticamente, senza l'intervento dell'utente finale, il protocollo più appropriato da utilizzare.

Yadis fornisce il primo passo per qualsiasi servizio che utilizza gli identificatori per l'autenticazione, autorizzazione, scambio di dati , e altro. Lo scopo di Yadis e quello di permettere al consumer (RP) di ottenere un file XRD (eXtensible Resource Descriptor). Per ottenere questo file il consumer effettua una richiesta HTTP. In risposta a tale richiesta il consumer (RP) può ottenere:

1. un documento XRD
2. un'url che contiene un file XRD valido.



La figura sotto mostra la “scatola nera” di Yadis che prende un URL come input e fornisce un documento XML come output..