L'IDENTITY MANAGEMENT

Le 3 A

È pratica consueta riferirsi all'insieme delle tecniche di autenticazione, autorizzazione e accounting come alle "3A". Il motivo di questo accostamento non risiede semplicemente nella condivisione della lettera iniziale, nonostante il forte gusto statunitense per questo tipo di giochi di parole, ma piuttosto nel ruolo coordinato e sinergico che questi tre aspetti della sicurezza IT rivestono all'interno del processo di protezione dei dati e dei servizi aziendali. Questi concetti riassumono le procedure e le funzioni necessarie per lo svolgimento di molti dei processi di sicurezza che avvengono sul Web. In un contesto di accesso geograficamente distribuito alle risorse informatiche è indispensabile, infatti, trovare dei metodi e delle regole in grado di garantire e proteggere il corretto svolgimento delle operazioni tra le parti che scambiano informazioni.

Le 3A sovrintendono proprio a questo tipo di funzioni. Più in particolare l'autenticazione è il processo per garantire in modo univoco l'identità di chi si appresta ad accedere alle risorse, l'autorizzazione definisce i privilegi di cui dispone questo utente, mentre l'accounting si riferisce all'analisi e alla registrazione sistematica delle transazioni associate a un'attività di business sul Web. La sicurezza di questi processi viene assicurata da una serie di tecnologie e procedure che si appoggiano su protocolli e standard e che costituiscono l'argomento di questo capitolo.

Implementare un sistema di autenticazione

I trend che alimentano il mercato delle tecnologie di autenticazione sono molteplici. Innanzitutto va consideratala continua espansione dell'accessibilità alle informazioni, legata alle nuove categorie di lavoratori mobili e da remoto nonché alla progressiva apertura del network delle grandi aziende verso partner e clienti. Inoltre cresce il numero di informazioni critiche e, conseguentemente, delle misure necessarie per controllare il loro accesso. A questi va aggiunta quella che si potrebbe definire come la "crisi delle password" ormai definitivamente abbandonate da tutti i principali fornitori di tecnologie in cerca di soluzioni più affidabili e meglio gestibili.

A controbilanciare questi argomenti concorrono aspetti quali i lunghi tempi di implementazione (trattandosi spesso di soluzioni che coinvolgono un grandissimo numero di utenti), i costi associati alla realizzazione di infrastrutture dedicate, ma anche la giustificazione dell'investimento rispetto ad altri ambiti tecnologici e di business,in un momento in cui i budget scarseggiano.

Resta in ogni caso il dilemma della scelta del sistema e della tecnologia da adottare tra i molti possibili e disponibili sul mercato, che variano dall'adozione di certificati digitali, alle smart card, ai token di vario tipo, alle credenziali virtuali o alle password, fino ad arrivare ai sistemi biometrici.

La risposta a quest'esigenza risiede nella valutazione di una serie di motivazioni che devono tenere in considerazione gli aspetti specifici di ogni azienda e dei suoi processi di business. Come sempre non esistono ricette uniche ma, di seguito, cercheremo di fornire alcuni spunti metodologici per orientarsi meglio in questo processo decisionale.

Il primo e fondamentale punto è quello di riconoscere che l'individuazione di una soluzione di autenticazione rappresenta un compromesso tra costi, sicurezza e praticità d'uso e che, pertanto, ogni decisione in merito dovrebbe essere presa come risultato di un'analisi di questi tre aspetti.

La cosa è complicata dal fatto che si tratta di parametri generalmente antagonisti fra loro: incrementare il livello di sicurezza determina costi proporzionalmente crescenti e una riduzione della flessibilità e semplicità d'uso perché richiede l'adozione di strumenti,procedure e tecnologie.

Un approccio metodologico dovrebbe partire da una metricizzazione di tali aspetti, inizialmente da un punto di vista qualitativo delle implicazioni e, se possibile, successivamente anche di tipo quantitativo. Per esempio è possibile individuare tutti gli aspetti significativi e correlarli attribuendo loro un indice numerico.

Anche se a qualcuno potrebbe sembrare un esercizio un po' accademico, l'adozione di una metodologia di questo tipo (o di altro analogo) permette di chiarirsi le idee su domande di difficile risposta quali: di quanta sicurezza ho effettivamente bisogno?

Non da ultimo, permette di facilitare la comprensione di determinate scelte tecnologiche anche da parte di chi mastica più il linguaggio del budget che quello tecnologico. Affrontare l'aspetto dei costi significa, ovviamente, considerare il Total Cost of Ownership della soluzione, che comprende non solo i costi di acquisizione, ma anche e soprattutto quelli di deployment e operativi, che vanno associati alle tecnologie, al personale, ai processi e alla struttura.

Eseguire un'analisi degli aspetti di sicurezza e praticità è, invece,il risultato di una valutazione strategica difficilmente ingabbiabile in regole. Tuttavia è possibile almeno separare gli aspetti legati al valore di una soluzione di autenticazione rispetto agli utenti e all'azienda.

La praticità e la semplicità d'uso, per esempio, dipendono, in generale, dalla tipologia di utenti che si stanno considerando e cambiano a secondo che si tratti di partner, dipendenti o clienti. Accanto alla complessità di apprendimento va considerata anche la praticità di utilizzo,che può inibire il suo impiego.

Anche gli aspetti legati alla trasportabilità della soluzione di autenticazione (indice importante della sua flessibilità) possono essere sensibilmente differenti in funzione della tipologia di utente e sono spesso legati a doppio filo con i costi. Per esempio, l'adozione di soluzioni che richiedono la presenza di un software sul lato client possono limitare l'accessibilità da aree esterne quali le filiali aziendali, un hotel o un chiosco pubblico. Un altro esempio può essere quello di soluzioni di autenticazione che sfruttano dispositivi mobili e che possono essere condizionate dall'area di copertura del servizio. Un ulteriore valore per l'utente può essere la versatilità. A volte il sistema di autenticazione può essere costituito da un dispositivo specifico, ma in altri casi può combinare in un unico dispositivo una pluralità di funzioni: sistema di autenticazione, documento di identità dotato di foto, strumento di memorizzazione di dati e così via.

Dal punto di vista della valenza strategica per l'azienda l'elemento primario da considerare è la sicurezza relativa, che deve tenere conto del livello di protezione offerto dal sistema di autenticazione , della sicurezza della sua implementazione, dall'adeguatezza a proteggere la tipologia di informazioni per cui lo si vuole utilizzare e anche della garanzia di compatibilità con la normativa.

A ciò va aggiunta la possibilità di integrazione all'interno dell'infrastruttura esistente e l'interoperabilità coni sistemi di back end.

In una valutazione non va, infine, trascurata la possibilità di lasciarsi aperte opzioni per le future evoluzioni tecnologiche. Un esempio in tal senso può essere quello dei certificati digitali,

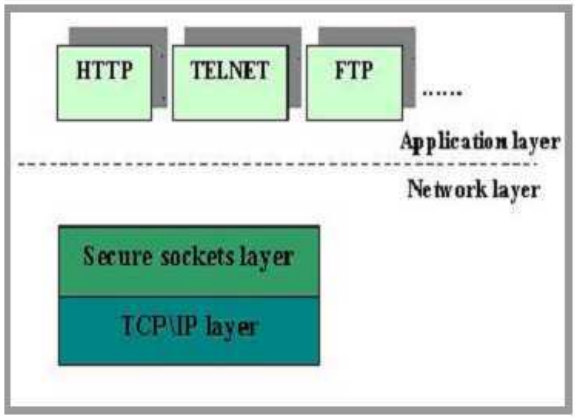
che rappresentano una soluzione utilizzabile inizialmente come sistema di autenticazione e che potrebbe essere adottata in futuro per la cifratura e per la firma digitale. Oppure di un sistema per l'autenticazione interna in grado di pubblicare asserzioni di identità che potrebbero essere utilizzate in seguito al di fuori dell'azienda.

I PRINCIPALI PROTOCOLLI DI AUTENTICAZIONE

Il protocollo SSL (Secure Socket Layer)

SSL è uno standard sviluppato specificatamente per la sicurezza su Internet. Ha subito nel tempo diversi aggiornamenti e ultimamente si è avuto il rilascio di una versione riferita con il nome di TSL (acronimo di Transaction Security Layer) ma anche con il nome di SSL versione 3.1 e pubblicata dall'IETF. È stata universalmente accettata nel mondo Web per le funzioni di autenticazione e di cifratura delle sessioni.

Come protocollo si posiziona sopra il TCP/IP e fornisce i servizi di encryption, autenticazione di server e client e autenticazione dei messaggi alle applicazioni soprastanti. Presenta la tipica struttura di un protocollo a livelli costituito da due layer principali, rispettivamente riferiti come l'Handshake Protocol e il Record Protocol. Quest'ultimo è responsabile dell'incapsulamento delle informazioni ricevute dai protocolli di più alto livello, mentre il protocollo di Handshake, che utilizza i messaggi definiti dal Record Protocol, ha il compito di creare la comunicazione tra il cliente il server.



Architettura a livelli dell'SSL
(Fonte RAD)

La realizzazione della connessione avviene mediante una reciproca autenticazione da parte del client e del server e tramite la negoziazione dell'algoritmo di cifratura da utilizzare e delle chiavi di cifratura.

SSL prevede il supporto di un ampio numero di metodi di cifratura:

- Crittografia simmetrica, come il DES o il triplo DES (3DES);
- crittografia pubblica, come RSA, DSS, KEA, utilizzata per autenticare l'identità del corrispondente. La chiave pubblica viene usata anche per determinare la chiave simmetrica che client e server useranno durante la sessione SSL.

Pur essendo un protocollo nato per Internet, in sé non è ristretto all'ambiente IP e può essere

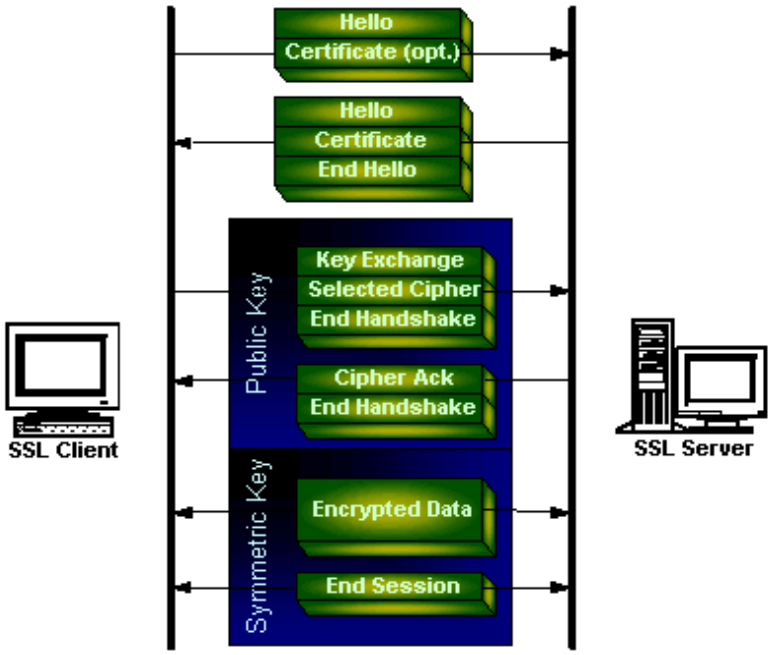
utilizzato anche in abbinamento ad altri protocolli di rete. Quando riceve dai livelli superiori i dati da trasmettere, li frammenta in blocchi, li comprime (se è prevista e concordata la funzione), applica al risultato un campo MAC (Message Authentication Code), cifra il tutto e trasmette il risultato. Sui dati ricevuti viene effettuato il procedimento inverso. I dati sono decifrati, verificati, eventualmente decompressi, riassemblati e passati al livello superiore.

Oltre ai due protocolli principali citati comprende altri elementi quali l'SSL Change Cipher Spec Protocol e SSL Alert Protocol. Il protocollo di Handshake e questi ultimi due hanno il compito di realizzare e gestire il setup della sessione e dei parametri di sicurezza. Le connessioni realizzate tra client e server sono associate a un'unica sessione, ma ogni sessione può includere connessioni diverse.

Lo stato di una connessione definisce i parametri MAC, mentre lo stato della sessione definisce un set di parametri di crittografia. Il protocollo di SSL Handshake, riferito anche come "key exchange protocol", ha la funzione di stabilire una connessione sicura tra le due parti interessate alla sessione.

Le fasi realizzate dal protocollo sono riassumibili in:

- autenticazione di server e Client (è opzionale);
- negoziazione dell'algoritmo di cifratura da utilizzare;
- utilizzo di una chiave pubblica per lo scambio dei parametri di cifratura.



Con riferimento alla figura, vediamo brevemente la funzione dei principali messaggi utilizzati dal protocollo:

- Client_hello: è inviato dal client per iniziare la sessione. Include al suo interno informazioni sul numero della versione SSL, un identificatore della sessione, informazioni sugli algoritmi di cifratura disponibili, un elenco degli algoritmi di compressione supportati.

- Server_hello: è il messaggio di risposta del server. Include i parametri visti per il client. Il server verifica che l'identificatore della sessione proposto dal client sia disponibile e, in caso contrario, ne propone uno alternativo tramite un'ulteriore fase di handshake. Il server sceglie poi un algoritmo per lo scambio delle chiavi di cifratura e le relative modalità nonché il metodo di compressione tra quelli proposti dal client. Server_certificate: è inviato dal server per autenticarsi nei confronti del client. Certificate_request: è inviato dal server quando vuole richiedere l'autenticazione da parte del client.

- Server_hello_done: viene inviato dal server per indicare che il server ha terminato quanto di sua competenza e cioè l'invio dei dati per la crittografia dei dati e i parametri di identificazione

- Client_certificate: è inviato dal client se il server ha richiesto al client la sua certificazione.

- Finished: è un messaggio inviato per indicare che la fase di set up si è conclusa positivamente.

A questo punto il protocollo di SSL Handshake completa i suoi compiti e sul canale privato e sicuro che si è stabilito possono essere trasferiti i dati delle applicazioni.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) è un protocollo definito dall'IETF per amministrare e rendere sicuro l'accesso remoto a una rete.

Il server software RADIUS include tre componenti:

- un server di autenticazione,

- protocolli per il client,

- un server di accounting.

Queste componenti possono girare su un'unica macchina oppure su dispositivi separati dotati di differenti sistemi operativi.

L'intero processo di funzionamento ha inizio quando un client crea un pacchetto RADIUS Access-Request, includendo almeno gli attributi User-Name e User-Password, e generando il contenuto del campo identificatore. Il processo di generazione del campo identificatore non è specificato nel protocollo RADIUS, ma è solitamente implementato come un semplice contatore incrementato ad ogni richiesta.

Il campo authenticator contiene una Request-Authenticator, ovvero una stringa di 16 byte scelta in modo casuale. L'intero pacchetto è trasmesso in chiaro, a parte per l'attributo User-Password, che è protetto nel modo seguente: il client e il server condividono una chiave segreta. Tale chiave viene unita con la Request Authenticator, e l'intera stringa viene sottoposta a una funzione hash MD5 per la creazione di un valore di 16 ottetti, sottoposto a sua volta a un XOR con la password immessa dall'utente (e se tale password è più lunga di 16 ottetti, vi è un calcolo MD5 addizionale, utilizzando il testo cifrato anziché la Request Authenticator).

Il server riceve il pacchetto Access-Request e verifica di possedere la chiave segreta per il client. In caso negativo, il pacchetto viene silenziosamente ignorato. Poiché anche il server è in possesso del segreto condiviso, è possibile utilizzare una versione modificata del processo di protezione del client per ottenere la password in chiaro. Quindi il server consulta il database per convalidare username e password; se la password è valida, il server crea un pacchetto Access-Accept da rimandare al client. In caso contrario, crea un pacchetto Access-Reject e lo invia al client.

Entrambi i pacchetti Access-Accept e Access-Reject utilizzano lo stesso valore identificatore del pacchetto Access-Request del client, e hanno una Response Authenticator nel campo Authenticator. La Response Authenticator è la funzione hash MD5 del pacchetto di risposta con l'associata Request Authenticator, concatenata con il segreto condiviso.

Quando il client riceve un pacchetto di risposta, si accerta che esso combaci con una precedente richiesta utilizzando il campo identificatore. Se non esiste alcuna richiesta con lo stesso identificatore, la risposta è silenziosamente ignorata. Quindi il client verifica la Response Authenticator utilizzando lo stesso calcolo effettuato dal server, ed infine comparando il risultato con il campo Authenticator. Se la Response Authenticator non coincide, il pacchetto è silenziosamente ignorato.

Se il client riceve un pacchetto Access-Accept verificato, username e password sono considerati corretti, e l'utente è autenticato. Se invece riceve un pacchetto Access-Reject verificato, username e password sono scorretti, e di conseguenza l'utente non è autenticato.

Utilizzo di RADIUS

RADIUS è un protocollo ampiamente utilizzato negli ambienti distribuiti. È comunemente usato per dispositivi di rete integrati come router, server modem, switch ecc., per svariate ragioni:

I sistemi integrati generalmente non riescono a gestire un gran numero di utenti con informazioni di autenticazione distinte, poiché questo richiederebbe molta più memoria di massa di quanta ne possiedano la maggior parte di essi.

RADIUS facilita l'amministrazione utente centralizzata, che è importante per diverse applicazioni. Molti ISP hanno decine di migliaia, centinaia di migliaia o anche milioni di utenti, aggiunti e cancellati di continuo durante una giornata, e le informazioni di autenticazione cambiano costantemente. L'amministrazione centralizzata degli utenti è un requisito operativo.

RADIUS fornisce alcuni livelli di protezione contro attacchi attivi e di sniffing. Altri protocolli di autenticazione remota offrono una protezione intermittente, inadeguata o addirittura inesistente.

Un supporto RADIUS è quasi onnipresente. Altri protocolli di autenticazione remota non hanno un consistente supporto da parte dei fornitori di hardware, quando invece RADIUS è uniformemente supportato. Poiché le piattaforme sulle quali è implementato RADIUS sono spesso sistemi integrati, vi sono limitate possibilità di supportare protocolli addizionali. Qualsiasi cambiamento al protocollo RADIUS dovrebbe quantomeno avere una compatibilità minima con client e server RADIUS preesistenti (e non modificati).

Nonostante ciò, è stato messo a punto un nuovo protocollo, Diameter, candidato a rimpiazzare RADIUS: utilizza infatti TCP anziché UDP ed è di conseguenza considerato più sicuro ed affidabile.