Lezione 13 modulo 1

Quando parliamo di autenticazione degli utenti, vogliamo riconoscere un utente che accede al nostro sistema, quindi il primo problema è il riconoscimento degli utenti. L'altro aspetto importante per quanto riguarda l'accesso ad un sistema da parte di un utente riconosciuto è sapere che diritti d'accesso ha questo utente: quindi abbiamo bisogno di associare i diritti d'accesso dell'utente al suo profilo di utente riconosciuto sul sistema. Quindi vogliamo consentire l'accesso ai dati e alle applicazioni. Qui stiamo parlando di un sistema informativo, quindi supponiamo che accedano al sistema degli utenti che vengono registrati sul sistema e quindi vediamo uno schema generale che potremo seguire per i vari passi che portano ad accedere l'utente ai suoi dati applicazioni. Quindi l'organizzazione, che è quella che si occupa della gestione di dati applicazioni nell'ambito del suo dominio di sicurezza, registra degli utenti sul sistema che, gli utenti, possono accedere al sistema tramite delle credenziali d'accesso che vengono appunto definite nel momento in cui l'utente viene registrato. Per quanto riguarda l'accesso al sistema e alle applicazioni, noi in generale assegniamo all'utente quello che viene chiamato un 'profilo dell'utente', quindi questo utente che viene riconosciuto, sarà riconosciuto ma sarà riconosciuto anche come un utente a cui ho assegnato un certo profilo che gli dà dei privilegi, quindi la possibilità di accedere ad alcune delle funzionalità del sistema. Quindi noi, una volta che un utente entrerà nel nostro sistema con le sue credenziali d'accesso, potremo andare a vedere quali privilegi ha questo utente e autorizzare l'accesso alle applicazioni e poi fare l'altra operazione di cui parleremo più avanti, che è il controllo dell'accesso ai dati che sono quelli a cui l'utente ha diritto ad accedere. Come possiamo effettuare il riconoscimento dell'utente? È chiaro che il modo più noto di accedere al sistema è quello dell'utilizzo di un login e di una password che conosce l'utente; questo nell'ambito della sicurezza viene chiamata la modalità 'Something you know', 'qualcosa che conosci', ed è chiaramente la modalità più comune di accesso al sistema. Non necessariamente però la conoscenza di qualcosa deve essere trasmessa in rete, ad esempio la password, non necessariamente viene trasmessa in rete ma possiamo anche utilizzare, oltre al sistema, abbiamo detto, login-password, anche dei sistemi ad esempio a sfida. Quindi l'utente con la conoscenza di quello che sa, quindi, appunto, una sua password che conosce, non restituisce la password, ma fa ad esempio delle elaborazioni dei dati che può fare solo perché è in possesso di questa conoscenza. Quindi quello che viene trasmesso poi in rete è questa elaborazione che consente di riconoscere l'utente perché ha potuto farla in base alla conoscenza che aveva. Questo ovviamente è un modo per riconoscere gli utenti che può essere soggetto ad attacchi e quindi ci sono altri meccanismi che sono stati sviluppati per rendere i sistemi più sicuri. Un altro modo comune di accedere a un sistema è 'Something you have'. Anche questo è abbastanza comune, pensate ad esempio all'accesso ad uno sportello bancomat, in cui dovete inserire non solo quello che sapete ma anche una carta per l'accesso allo sportello. In alcuni sistemi è necessario anche un livello superiore di sicurezza e quindi vengono utilizzati dei metodi di riconoscimento basati sul riconoscimento di caratteristiche fisiche della persona. Questa è un'altra categoria chiamata 'Something you are', ad esempio possiamo riconoscere l'iride, dei punti delle impronte digitali in modo da riconoscere appunto la persona sulla base di alcune caratteristiche fisiche. Anche questo è un metodo che si sta diffondendo anche nell'ambito dell'utilizzo di dispositivi mobili, ad esempio i cellulari. Questo riconoscimento dell'utente, come abbiamo detto, ci consentirà di capire che utente è entrato nel sistema e poi andiamo a dare i privilegi a cui ha diritto sul sistema.