Protezione dei file, autenticazione di utente

Lezione 16 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2006-7

Indice

protezione dei file

protezione dei file nei primi sistemi operativi:
piuttosto rudimentale, dicotomica (tutto o niente, tutti o nessuno)

l'avvento del **time sharing** e della **multiprogrammazione** sollecitano forme più articolate di protezione:
definizione di **tipi di diritti di accesso**, che classificano le operazioni sui file, ad es. rwx nel sistema Unix
definizione di **gruppi di utenti**
autorizzazione per tipi di diritti di accesso a: proprietario, gruppo, mondo

un aspetto che differenzia modelli di autorizzazione in sistemi diversi è se un utente possa appartenere a **più gruppi:**
ciò è possibile nei sistemi in cui prevalgono le esigenze della **condivisione**
il contrario caratterizza invece i sistemi in cui la sicurezza è più marcatamente basata sulla **separazione**

i sistemi Unix offrono inoltre la possibilità di **autorizzazione procedurale dinamica** mediante set user-id (**suid**) e set group-id (**sgid**), che esaminiamo appresso

protezione procedurale

in un sistema Unix le password degli utenti sono memorizzate, in forma crittografata, in un file modificabile solo dall'amministratore ... tuttavia, ogni utente può modificare la propria password senza dover scomodare l'amministratore (che ha certo di meglio da fare ;)

problemi:
1. come riesce l'utente a modificare un file la cui modifica è permessa solo all'amministratore?
2. cosa gli impedisce di modificare le password di altri utenti (magari a loro insaputa)?

soluzione: protezione procedurale con autorizzazione dinamica

i diritti di accesso ai file che un processo in esecuzione ha nei sistemi Unix sono quelli assegnati al suo user-id, che normalmente è quello dell'utente che lo ha lanciato

è però possibile conferire a una procedura eseguibile la protezione **suid**, che ne determina l'esecuzione con l'user-id del suo proprietario invece che dell'utente che la lancia

questo meccanismo permette di risolvere agevolmente entrambi i problemi proposti:
1. l'utente modifica il file delle password eseguendo una procedura dell'amministratore con protezione **suid**: ciò gliene conferisce i privilegi, ma **solo nell'esecuzione di tale procedura**
2. la procedura funge da scudo fra l'utente e il file, del quale esegue una **modifica controllata**

la protezione **sgid**, funziona in modo analogo per i diritti di accesso assegnati al gruppo, ed è adoperata ad es. in sistemi di collaborazione in rete

elementi per l'autenticazione di utente

gli elementi disponibili a un sistema operativo per accertare la veridicità dell'identità di un utente possono essere classificati in tre categorie, in quanto basati su ciò che l'utente

conosce: password, PIN, chiave segreta di cifratura, ...

ha: badge, documenti di identità, chiavi fisiche, ...

è: caratteristiche biometriche quali: impronte digitali, voce, mappa della retina, geometria delle mani, DNA, ...

garanzie migliori di autenticazione possono spesso ottenersi da una **combinazione** di elementi, dello stesso tipo o di tipi diversi

ad es., alcuni sistemi di autenticazione per l'accesso telematico ad operazioni bancarie richiedono la conoscenza di un PIN e di una password usa-e-getta, generata da un dispositivo in possesso del titolare del conto

autenticazione mediante password

nei sistemi operativi è il metodo di autenticazione di utente più comune

è altresì molto comune per l'autenticazione di utenti di **servizi** forniti da software applicativo:

ad es., posta elettronica, basi di dati, siti Web ad accesso riservato, ...

per la memorizzazione delle password è di largo impiego l'uso della **crittografia**

tale protezione può risultare tuttavia insufficiente se la **trasmissione** della password, ad es. all'inizio di una sessione di lavoro, non gode di simile protezione

l'impiego di validi meccanismi di crittografia sia per la memorizzazione che per la trasmissione di password non pone però al sicuro dalla più formidabile fonte di vulnerabilità della protezione mediante password: l'**utente...**

alcuni sistemi applicano restrizioni e controlli sulla scelta della password da parte degli utenti, per evitare che questa risulti troppo facilmente attaccabile

ad es., troppo breve, derivata dal nome dell'utente, termine comune da un dizionario, ...

dispositivi di autenticazione

l'impiego di dispositivi fisici per l'autenticazione non è frequente per l'accesso ai sistemi operativi, ma si sta rapidamente diffondendo per **applicazioni specifiche** che, grazie alla contemporanea diffusione dei sistemi informatici, richiedono spesso supporti hardware e software funzionali a tal fine

> ad es., nel sistema di autenticazione per la firma elettronica dei verbali di esame nel nostro ateneo, il docente dispone di una smart card e di una password, e può apporre la firma digitale solo da una postazione remota che sia dotata del dispositivo di lettura richiesto e in cui siano installati i driver per questo

il proliferare dell'impiego di schede digitali per l'accesso ai servizi più disparati (credito, commercio, sanità, etc.) motiva la ricerca, da parte delle organizzazioni più grandi, di meccanismi di **integrazione** che permettano l'accesso a una pluralità di servizi con uno stesso dispositivo

autenticazione biometrica

l'accertamento dell'identità da caratteristiche fisiche della persona ha una storia antica

> dopo tutto, fra esseri umani ci si riconosce dal volto o dal timbro della voce sin dalla prima infanzia, dai tempi più antichi

qualità di caratteristiche biometriche rilevanti all'autenticazione:
facilità d'uso, discriminazione (false accettazioni, falsi rifiuti), rapidità, falsificabilità

> le impronte digitali offrono una discriminazione accettabile (frequenza di errore non oltre il 10%), ma sono falsificabili con la gelatina
> l'impronta retinica ha un'ottima discriminazione, ma richiede un fascio di luce diretto sull'occhio per il rilievo della mappa dei vasi sanguigni, il che causa disturbo
> lo schema dell'iride presenta una discriminazione inferiore, ma può essere rilevato da una comune macchina fotografica
> molto promettenti sono le tecniche basate sul DNA: due esseri umani differiscono nell'1 per mille della sequenza di nucleotidi che forma la molecola, ma questa ne conta circa 3 miliardi, dunque la discriminazione è potenzialmente assoluta

per una panoramica introduttiva più completa si rinvia alla relazione (Maggiorelli, 2006)

autenticazione in rete

al proliferare dei servizi disponibili in sistemi informatici e in rete corrisponde una naturale proliferazione delle interazioni di autenticazione, e delle password che ogni utente deve custodire

per contrastare questa tendenza si cerca di realizzare sistemi di **autenticazione singola**, ingl. Single Sign-On (SSO), nei quali il servizio di autenticazione, stabilita la sessione, fornisce l'identità autenticata dell'utente ai processi che la richiedono

- servizi di directory, quali LDAP o X.500, possono essere utilmente impiegati per realizzare l'autenticazione singola

una debolezza intrinseca dei sistemi di autenticazione singola sta nel fatto che inevitabilmente danno luogo, almeno per ogni utente, a una vulnerabilità **critica**

- il successo di un attacco all'informazione di SSO crea una breccia di ampiezza proporzionale all'uso che l'utente fa del servizio

una ragion d'essere analoga hanno gli onnipresenti **cookie** di autenticazione

- programmi installati nel browser, che sollevano l'utente dalla necessità di ricordare le credenziali di autenticazione per servizi di rete già visitati

i cookie possono però fare altro, ad insaputa dell'utente...

- ad es., raccogliere statistiche sulle sue abitudini di esplorazione in rete, in forma aggregata e anonima nella non peggiore delle ipotesi

riferimenti

Maggiorelli (2006) :

Relazione sulle metodologie di identificazione attraverso la tecnologia biometrica

Contributo al corso di Sicurezza dei sistemi informatici 1, Comiso (RG)