Utente Password

La sicurezza di un sistema informatico comincia decidendo chi può fare che cosa. Amministrare la sicurezza significa creare un certo numero di utenti e per ognuno di essi decidere a quali dati può accedere e quali può modificare. Il sistema riconosce gli utenti utilizzando una coppia di stringhe: utente, password. Per evitare che sia troppo semplice attivare uno scambio di persona (utente) le password dovrebbero essere gestite rispettando una serie di regole:

- Lunghezza di almeno 8 caratteri. Il numero di combinazioni aumenta esponenzialmente con il numero dei caratteri quindi anche il computer più potente impiegherebbe un tempo troppo lungo per provare con tutte le combinazioni possibili.
- Inserire cifre, lettere minuscole e maiuscole, sempre per aumentare il numero di combinazioni possibili
- Evitare stringhe con significati precisi, date, nomi, luoghi in modo che l'utilizzo di "vocabolari" non dia alcun vantaggio a chi si vuole impadronire della password
- Cambiare periodicamente (3 mesi) la password per evitare che qualcuno osservandovi riesca a registrare la sequenza di tasti premuta
- Evitare di scrivere la password su foglietti facilmente accessibili o addirittura in vista.

LDAP

Le informazioni sugli utenti e i relativi permessi sono registrati in un database LDAP (Lightweight Directory Access Protocol) con una struttura ad albero come le cartelle del file-system.

Esempi di implementazioni di questo database sono:

- **Active Directory** di Microsoft
- **OpenLDAP** in Linux

Virus

La maggior parte dei problemi di sicurezza sono legati all'attività automatica di programmi informatici specializzati detti virus. Semplificando molto un virus è una serie di istruzioni (non un programma completo) in grado di fare due cose:

1. Duplicarsi in un programma presente nel PC diffondendo cosi l'infezione.
2. Attivarsi per svolgere un compito specifico. Danneggiare o rallentare il PC, leggere dati riservati come password di carte di credito o di conti correnti, acquisire il controllo del PC infettato

I principali canali di diffusione sono:

- Internet in particolare gli script presenti nelle pagine Html
- Gli allegati di posta elettronica che possono contenere macro o istruzioni VBA
- Programmi eseguibili

Affinché un virus si attivi è necessario che il programma che lo contiene sia eseguito sul computer, per questo è buona norma disabilitare l'anteprima dei file che presuppone una esecuzione del codice.

Va inoltre evitato l'uso del computer con i privilegi di amministratore. Il programma infetto va in esecuzione con gli stessi permessi dell'utente collegato, se questo non può fare certe operazioni automaticamente le stesse limitazioni saranno applicate al virus che non potrà ad esempio modificare nessun file di sistema.

E' indispensabile l'installazione di un antivirus da tenere costantemente aggiornato. Consigliabile anche una scansione periodica completa del PC.

Crittografia a chiave pubblica.

Esistono programmi per generare una coppia di chiavi in relazione fra di loro, una parte è **pubblica** e distribuibile liberamente, l'altra parte è **privata** e va custodita gelosamente. Nelle **chiavi simmetriche** si usa la stessa chiave per codificare e decodificare, in questo caso si tratta di una chiave **asimmetrica** con chiavi diverse per codifica e decodifica. Esistono due tipi di utilizzo: l'autenticazione e la crittografia.

Autenticazione

L'autore usa la sua chiave privata per firmare un documento o un messaggio, in pratica si aggiunge la firma al documento. Il lettore con parte pubblica della chiave è in grado di sapere se il documento è effettivamente dell'autore e nella sua forma originale. Il sistema è sicuro nella misura in cui si ha la certezza che la chiave pubblica è effettivamente dell'autore. La stessa coppia di chiavi può essere usata più volte e su più documenti.

Non è possibile usare lo stesso canale per trasmettere il messaggio e la chiave pubblica. Un malintenzionato potrebbe modificare il documento originale, generare la coppia chiave pubblica-privata, firmare il documento e trasmetterlo assieme alla chiave appena generata. **E' essenziale attivare un canale sicuro per trasmettere la parte pubblica della chiave.**

X.509

X.509 è uno standard per la distribuzione dei certificati che contengono anche una chiave pubblica oltre ai dati dell'autore che firma con la sua chiave privata.

Crittografia

Con la crittografia si vuole che il messaggio o il documento possa essere letto solo dal destinatario. Chiunque altro possa acquisire una copia potrà vedere solo informazioni non comprensibili.

La parte pubblica della chiave può essere usata per crittografare un documento. La lettura del documento può essere fatta solo con l'uso della chiave privata. L'uso di chiave pubblica e privata è poco efficiente per la crittografia dove sono più convenienti le chiavi simmetriche uguali per la cifratura e la decifratura ma meno sicure.

Nella pratica si usa la coppia chiave pubblica-privata per la trasmissione della chiave simmetrica da usare per la codifica della trasmissione. Ad ogni nuova sessione si può in questo modo generare una nuova chiave simmetrica di cifratura per avere sempre la massima sicurezza.

Un amministratore rende disponibile la sua chiave pubblica in internet e conserva la parte privata con la massima accuratezza.

- Chi vuole comunicare genera una chiave simmetrica, la codifica con la parte pubblica della chiave e la trasmette all'amministratore.
- Solo l'amministratore può decifrare la chiave simmetrica usando la parte privata della chiave.
- La trasmissione avviene crittografando con la chiave simmetrica che in nessun momento è stata trasmessa in chiaro.

Secure Sockets Layer (SSL)

SSL permette di stabilire una **connessione sicura** (crittografata e senza scambio in chiaro della password) con siti internet o con server SQL basandosi sull'utilizzo di certificato asimmetrici con chiave pubblica-privata per la trasmissione della chiave simmetrica da utilizzare per tutta la sessione.

Telnet

E’ un servizio, solitamente sulla porta 23, per il controllo remoto di un server in modalità testo. Attualmente in disuso in quanto il traffico è in chiaro compresa la password di autenticazione.

SSH

Secure Shell (shell sicura). Ha sostituito Telnet nell’amministrazione remota dei server in quanto il traffico è crittografato ed è prevista anche un’autenticazione del server.

PuTTY è un client SSH freeware che permette la gestione di host remoti.