1-08-08 (rivedere esercizio 6)
- Discutere i principali approcci che possono essere usati per autenticare gli utenti, evidenziando i loro vantaggi e svantaggi.
***
Autenticazione basata sulla conoscenza:
1)autenticazione basata su password:basata su coppia login,password;semplice,economico,facile da implementare, ma anche il + debole.VulnerabilitÃ
delle password: possono essere facilmente indovinate..bruteforce..ecc.
2)Basata sul possesso:Ogni token ha una chiave crittografica memorizzata nel token, usata per dimostrare l'identitÃ del token ad un pc.Sono + sicuri
delle password.VulnerabilitÃ : possono essere persi o rubati.Chiunque acquisisce un token puÃ² impersonare l'utente. (memorycard, smart token).
3)Autenticazione basata su caratteristiche:caratteristiche biometriche.Fisiche e comportamentali.(firma, voce ecc..).Vantaggi:sicure, difficilmente
replicabili.Svantaggi:Costose, intrusive, non tutelano la privacy.
****

- Descrivere il concetto di Trojan Horse e fornire un esempio di come un Trojan Horse pu`o violare le restrizioni imposte da una politica discrezionale. Descrivere inoltre perchÂ´e tale Trojan Horse fallirebbe in presenza di una politica multilivello.
****
programma che svolge la funzione di utilitÃ ma che in realtÃ compie sul sistema all'insaputa dell'utente operazioni dannose.
Un trojan horse in un contesto di politica discrezionale puÃ² scalare i privilegi in base alle politiche di restrizione imposte sull'utente violato.
Un trojan horse infettando programmi di un utente riceve (secondo la politica discrezionale) tutti i privilegi associati all'utente stesso.
In presenza di politica multilivello, fallirebbe perchÃ¨ utenti di livello alto possono eseguire tutte le operazioni su utenti di livello inferiore ma
il contrario nn Ã¨ possibile.
****
- Descrivere la differenza tra utenti e soggetti nelle politiche mandatorie.
****
utenti=persone.
Soggetti = Processi (programmi in esecuzione). Operano per conto degli utenti.
****
- Descrivere lo smurf attack, come funziona e possibili contromisure.
****
Lo smurf attack sfrutta le debolezze del protocollo ICMP e punta al Denial of Service (DoS) di un host. L'attacco consiste di due fasi : fare lo
spoofing dell'indirizzo IP che si vuole attaccare e poi mandare un ping in broadcast. A questo punto tutti gli host delle rete broadcast invieranno
una risposta all'indirizzo spoofed provocando il DoS.Per difendersi da questo tipo di attacco bisogna rifiutare il broadcast IP interface serial.
****
- Descrivere la vulnerabilit`a delle stringhe di formato e fornire un esempio.
****
In breve, si tratta di passare a una funzione che stampa una stringa a schermo, tipicamente una printf del linguaggio C, una stringa che in realtÃ
contiene una serie di parametri di specifica dell'input (tipicamente si usano gli specificatori di formato %s e %x per esaminare il contenuto della
memoria e %n per sovrascrivere parti della memoria, in particolare dello stack, questo permette attacchi di tipo stack overflow e return to libc). In
pratica, quando si vuole stampare una stringa s usando la printf() o un'altra funzione C che accetta un numero illimitato di specificatori di
formato, bisogna scrivere la funzione printf("%s",StringPointer) e non printf(StringPointer).
****
- Descrivere il processo di autenticazione di PGP.
****
Ã¨ un software di crittografia per la posta elettronia e la protezione di file di uso personale.Permette di firmare una email lasciando il testo in
chiaro, permette di cifrare una email senza firmarla, permette di fare entrambe le cose.L'autentificazione avviene tramite una funzione hash.

Lato Mittente: Il messaggio in chiaro viene crittato tramite una funzione hash ed a quest'ultimo viene associata la chiave privata del mittente. Come
terzo passaggio il risultato di questa unione viene assimilato con il messaggio in chiaro originale. Il risultato viene compresso e spedito al
destinatario.
Lato Destinatario: il messaggio crittato viene decompresso e suddiviso in due parti, una contenente il messaggio in chiaro e l'altra contenente la
firma. Al messaggio in chiaro viene applicata la funzione di hash, mentre alla firma viene associata la chiave pubblica del mittente. L'operazione
finale Ã¨ il confronto tra le due parti.
****
- Nellâ€™ambito delle politiche per il controllo dellâ€™accesso, caratterizzare il principio del minimo privilegio (least privilege) e spiegare la differenza fra gruppi e ruoli.
Il principio del minimo privilegio limita la possibilitÃ di abusi e danni per violazioni perchÃ¨ assegna il privilegio minimo a tutti gli utenti cosÃ¬
facendo non si puÃ² intaccare il sistema.(spiegare i danni di questa politica). I gruppi raggruppano utenti(statici) i ruoli invece raggruppano
privilegi(dinamici).
****
- Data una politica ChineseWall dove i company dataset sono BankA, BankB, OilA, OilB e le classi di conflitto di interesse
sono CoI1 = {BankA, BankB} e CoI2 = {OilA, OilB}, si supponga che un soggetto S1 esegua una operazione di lettura su un oggetto del dataset BankA ed un oggetto del dataset OilB. Si richiede di indicare i dataset che contengono oggetti che S1 pu`o scrivere e di motivare la risposta.
??
??'"
??
??
****
- Nellâ€™ambito dei sistemi operativi Unix-based, descrivere il significato dei privilegi setuid e setgid.
SetUid imposta il valore intero unico per ogni UTENTE(login name, etc/shadow). SetGid imposta il GRUPPO all'utente. Ogni utente Ã¨ membro di un gruppo
primario identificato da un numero (etc/group).
****
- Descrivere il metodo basato sulla matrice delle risorse condivise per lâ€™identificazione di covert channel. Illustrare inoltre
un esempio di possibile canale che pu`o essere scoperto tramite tale tecnica.
Metodo: Si costruisce una matrice M dove le righe sono le risorse, le colonne e i processi -M[i,j] = R se il processo j puÃ² leggere o osservare la
risorsa i. -M[i,j]=M se il processo j puÃ² modificare, creare, cancellare la risorsa i. Si cerca la presenza di due colonne e di due riche che
mostrano il pattern con la M incrociata tra due R e successivamente si completa la matrice con il flusso potenziale di informazione. Si analizza
infine la matrice per verificare se ci sono flussi di informazione indesiderati. Si possono scoprire f/|lussi di informazione non ovvi tra le
istruzizoni di un programma. Per esempio: -B := A realizza un flusso di informazione da A a B (flusso esplicito) -If D=1 then B:=A realizza due
flussi, da A a B ma anche da D a B (flusso implicito).
****
- Illustrare in modo dettagliato e preciso come la stringa di formato %n pu`o essere utilizzata per sovrascrivere lâ€™indirizzo
RET nello stack.
****
- Nellâ€™ambito del modello a matrice di accesso, dare la definizione di transizione di stato ed enunciare in modo preciso e
formale il problema della safety.
L'attaccante inserisce %n dove il numero di carateri in stinga deve essere uguale all'indirizzodello stack dove inizia il codice maligno.
Sovrascrive lo stack con l'indirizzo RET printf(buffer) scrive il numero di caratteri in stinga in RET
****
- Dare la definizione di virus crittografico e descrivere le tre parti principali di cui tale tipo di virus solitamente si compone.
Un virus crittografico Ã¨ un virus polimorfo che sfrutta tecniche crittografiche per cambiare forma. Contiene 3 parti:

chiave di decrittazione (varia
a seconda dell'infezione). Codice crittato. Routine(non crittata) per la decrittazione del codice. La routine puÃ² esere considerata come signature
del virus.
****
- Nellâ€™ambito del sistema Kerberos, dire quali sono i tre compiti principali dellâ€™Authentication Server (AS) ed i tre compiti
principali del Ticket Granting Server (TGS).
Per quanto riguarda AS i compiti principali sono:1)fornire un servizio di autenticazione.2)Conosce le password di tutti gli utenti.3)Condividere una
chiave segreta univoca con ciascun server.Per TGS 1)fornire un controllo dell'accesso.2)Genera un ticket di servizio per gli utenti che sono stati
autenticati da AS.3) Ticket di servizio utilizzato per accedere ad un determinato servizio offerto da un server.
****
- Nellâ€™ambito dei sistemi per la determinazione di intrusioni, dire cosa si intende per falsi negativi e r .
Falso positivo attivitÃ non intrusiva ma anomala, falsi negativi attivitÃ anomala ma non intrusiva
****
1. In base alla politica Chinese wall un soggetto pu`o trovarsi in una situazione in cui non `e pi`u in grado di eseguire alcuna operazione di scrittura. Si richiede di descrivere un semplice esempio che illustri questa situazione (lâ€™esempio deve includere i dataset presenti nel sistema ed i relativi oggetti e le classi di conflitto di interesse).
??????????????????????????????"
??????????????????????????????
??????????????????????????????
****
2. Si richiede di definire il principio del minimo privilegio. Lâ€™account root nei sistemi operativi Unix-based viola questa privilegio? Motivare la risposta.
Nel principio del minimo privilegio Ã¨ opportuno che le utenze abbiano i soli diritti necessari al normale svolgimento delle attivitaâ€™ di competenza.
Si, l'utente root quindi viola questo privilegio.
****
3. Nei sistemi operativi Unix-based la password prima di essere memorizzata viene combinata con un sale. A cosa serve il sale? Lâ€™uso del sale rende eventuali attacchi allâ€™account di uno specifico utente pi`u difficili rispetto ad attacchi simili eseguiti in sistemi dove il sale non viene usato? Motivare la risposta.
Due utenti con la stessa password hanno entrate identiche nel file delle password. Questo permette agli utenti di conoscere l'uno la password
dell'altro. Nei sistemi unix si evitano queste situazioni usando una tecnica chiamata SALE. Ã¨ composta da 12 bit unica per ciascun utente e
memorizzata in chiaro. La crittazione avviene applicando una funzione di hash all'unione dei 56 bit della password in chiaro e dai 12 bit del sale.
Restituisce in output 11 caratteri. Ovvio che un attacco viene reso molto piÃ¹ difficoltoso con l'ausilio del sale.
****
5. Descrivere il processo di creazione di un certificato digitale.
Un utente prova la propria identitÃ alla CA(autoritÃ di certificazione) dove le procedure non sono crittografiche. CA verifica l'integritÃ della
chiave(coppia chiavi pubblica/privata generata dalla CA) e (coppia chiavi pubblica/privata generata dall'utente). CA crea un certificato digitale che
contiene la chiave pubblica ed i dati identificativi dell'utente. CA firma il certificato digitale con la propria chiave privata.
****
7. Descrivere in modo preciso, illustrando anche il contenuto dello stack, in cosa consiste un attacco di overflow dello stack.
Uno stack overflow Ã¨ la scrittura al di fuori dei limiti della memoria assegnata allo stack che si va a sostituire alle istruzioni del programma in
esecuzione. Si immagini l'utilizzo di una allocazione di memoria dedicata all'esecuzione di un programma come una pila. Mentre le istruzioni vengono
allocate in quell'area partendo dall'alto verso il basso della pila, lo stack, utilizzando la sua organizzazione LIFO, crescerÃ dal basso verso
l'alto di questa seguendo quanto indicato dallo stack pointer, un registro dedicato delle CPU.Opportunamente sfruttato questo tipo di overflow puÃ²
far si che un utente malintenzionato sfrutti questa vulnerabilitÃ per l'esecuzione di codice arbitrario che si va a sostituire a quello del programma
in esecuzione.
****

1. Nellâ€™ambito degli attacchi a protocolli di rete, descrivere in maniera chiara e sintetica in cosa consiste un attacco di tipo Denial-of-Service (DoS). Quali sono le differenze tra DoS e DDoS (Distributed Denial-of-Service)? Nell'attacco DoS il sistema nega (per
errore) l'accesso ai servizi/informazioni anche ad utenti regolarmente autorizzati. Il principio su cui si basa l'attacco Ã¨ semplice: -inondare di
richieste casuali la macchina obbiettivo dell'attacco.-il target dell'attacco non riuscirÃ + a supportare il carico di richieste e quindi smetterÃ di
funzionare. Si differenzia dal DDOS Ã¨ che in quest'ultimo ci sono agenti(zombi) in numero elevato, distribuiti su differenti computer e sincronizzati
da pochi centri(master). -Gli utenti delle macchine zombie sono ignari di essere strumenti usati per l'attacco DDOS. I master sono macchine infettate
oppure di proprietÃ dell'attaccante. Quest'ultimo invia messaggi ai master che a loro volta inviano agli zombi per cominciare l'attacco. il DDOS Ã¨
diviso in due fasi: infettare le macchine primarie e poi attacco vero e proprio mentre il dos non si compone della prima parte.
****
2. Nellâ€™ambito delle tecniche di autenticazione basate su caratteristiche dellâ€™utente, descrivere in cosa consiste la
fase di enrollment.
Al fine di verificare l'identitÃ di un individuo tramite un sistema biometrico, Ã¨ necessario procedere a una fase iniziale di registrazione
(enrollment), durante la quale vengono acquisite una o piÃ¹ istanze della caratteristica biometrica. Da quest'ultima ne vengono estratte le
caratteristiche discriminanti e viene costruito il modello dell'utente â€“ PiÃ¹ misurazioni della caratteristica di interesse â€“ Definizione di un
template
****
3. Descrivere le caratteristiche principali delle politiche discrezionarie. PerchÂ´e sono politiche discrezionarie?
Le politiche discrezionarie controllano lâ€™accesso sulla base dellâ€™identita degli utenti che lo richiedono e su regole che stabiliscono chi puo (o non
puo) eseguire azioni sulle risorse. Sono chiamate discrezionarie perche agli utenti puo essere data lâ€™autorita di passare i propri privilegi ad altri
utenti (la concessione e la revoca di privilegi e controllata da una politica amministrativa).
****
4. Nellâ€™ambito delle politiche mandatorie per la protezione dellâ€™integrit`a, spiegare i principi no read down e no write up e fare un esempio di lettura e scrittura che non sono permesse in base a tale politica.
No write down un soggetto s puo scrivere solo oggetti la cui classificazione domina quella di s (Î»(o) >= Î»(s)).
Utenti ad alto livello si possono collegare a livelli piu bassi per scrivere informazioni non sensibili.
No read up un soggetto s puo leggere solo oggetti o la cui classificazione e dominata da quella di s (Î»(s) >= Î»(o)).
Gli oggetti creati prendono la classificazione del soggetto che li ha creati.
********** `
6. Dire cosa si intende per storage channel e fornire un esempio.
Sono canali coperti che sfruttano la presenza o l'assenza di oggetti in memoria. Un esempio Ã¨ il canale detto file lock: -in un sistema multi utente
si usa un meccanismo di lock che impedisce piÃ¹ modifiche allo stesso file. - Un canale nascosto puÃ² segnalare un bit di informazione sfruttando il
fatto che un file puÃ² essere bloccato (locked) oppure no.
****
7. Descrivere il processo di handshake del protocollo SSL.
++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++
+++++++vedere pag 84...
****
8. Descrivere cosa rappresenta una relazione di associazione del protocollo IPSec.
Costituisce la base del funzionamento di IPsec. Una SA (security association) Ã¨ un "contratto" fra le due entitÃ coinvolte nella comunicazione; in
essa vengono stabiliti i meccanismi di protezione e le chiavi da utilizzare durante il successivo trasferimento dei dati.E' identificata da:
-security parameters index;-indirizzo IP destinazione;-identificatore del protocollo di sicurezza. Contiene:-sequence number counter;-sequence
counter overflow;-anti-replay window;-informazione AH;-informazione ESP;-lifetime;-modalitÃ trasporto;-path MTU.

****
2. Nellâ€™ambito del modello di Bell e LaPadula, descrivere la tranquility property e fare un esempio del perchÂ´e `e necessario introdurre tale propriet`a.
Il sistema Ã¨ modellato come stati e transizioni di stato.Il livello di sicurezza degli oggetti non puoâ€™ cambiare se non con regole precise.
??
??
****
3. Descrivere il buffer overflow illustrando anche un esempio.
Il buffer overflow Ã¨ una vulnerabilitÃ di sicurezza che puÃ² affliggere un programma software. Consiste nel fatto che tale programma non controlla in
anticipo la lunghezza dei dati in arrivo, ma si limita a scrivere il loro valore in un buffer di lunghezza prestabilita, confidando che l'utente (o
il mittente) non immetta piÃ¹ dati di quanti esso ne possa contenere: questo puÃ² accadere se il programma Ã¨ stato scritto usando funzioni di libreria
di input/output che non fanno controlli sulle dimensioni dei dati trasferiti.Esempio:
|strcpy(record,user); |
|strcat(record,":"); | Copia username("user"nel buffer("record"),appende ":" e l'hash della password ("cpw")
|strcat(record,cpw); |
SOLUZIONE
strncpy(record,user,MAX_STRING_LEN-1);
strcat(record,":");
strncat(record,cpw,MAX_STRING_LEN-1);
****
4. Nellâ€™ambito delle politiche mandatorie per lâ€™integrit`a, spiegare i principi in base ai quali si verofica se le operazioni
di letture e scritture possono essere permesse, supponendo di applicare una politica: i) low water mark
per oggetti; ii) low water mark per soggetti.
??????????????????????????????
??????????????????????????????
****
6. Dire cosa si intende per SQL injection, fare un esempio ed illustrare in che modo `e possibile difendersi da questa tipologia di attacco.
Interessa qualsiasi linguaggio di programmazione e qualsiasi dbms.Interrogazioni SQL costruite sulla base di input passati da un utente possono
essere manipolate a piacimento.-Input trasmesso in vari modi:-tramite URL(query string).-Tramite un form HTML.-Tramite cookie costruito su
misura.CONTROMISURE:Controlli sul tipo di dato;creazione di filtri tramite espressioni regolari;eliminazione di caratteri potenzialmente
dannosi;escape di caratteri potenzialmente dannosi.ESEMPI:$sql="SELECT * from Utenti where login='$login' AND password='$password'" La query puÃ²
essere modificata manipolando $login che potrebbe essere "pippo" OR "1=1 --"
7. Nellâ€™ambito dei meccanismi per il controllo dellâ€™accesso, elencare e spiegare le cinque caratteristiche base di un
reference monitor .
##########
##########
##########
****
3. Descrivere le tre tipologie di asserzioni che possono essere definite in SAML.
SamlAction, Rappresenta l'elemento <saml:Action> all'interno di un'asserzione SAML che contiene un'azione su una risorsa specificata.
SamlAdvice, Rappresenta l'elemento <saml:Advice> all'interno di un'asserzione SAML che contiene informazioni aggiuntive fornite dall'autoritÃ SAML.
SamlAssertion, Rappresenta un'asserzione SAML (Security Assertion Markup Language
****
4. Descrivere lâ€™attacco ping of death.
Basato sul protocollo ICMP, i pacchetti ICMP hanno un payload la cui dimensione Ã¨ superiore a un ceto valore, il sistema che riceve questi pacchetti
va in cresh.
****
6. Si supponga di avere a disposizione un web server Apache. Si richiede di definire delle regole di controllo dellâ€™accesso

che permettano lâ€™accesso al contenuto della directory /usr/pippo/www solo allâ€™utente esame05 (esame05 `e la login
dellâ€™utente) le cui richieste di accesso possono essere accettate solo se provengono dalla macchina con IP 134.123.786.9.
::r0x::
Bisogna lavorare sul file .htaccess inserendo le seguenti regole:
Order Deny,Allow
Deny from all
Allow from 134.123.786.9
E sul file .htpassword
inserendo le seguenti regole:
AuthType Basic
AuthName "Rescricted Area"
AuthUserFile /usr/pippo/www
require user esame05
****

7. Descrivere le tre principali minacce alla sicurezza di e-mail.
Le tre principali minacce sono: -perditÃ di confidenzialitÃ :(-e-mail spedita in chiaro su una rete non sicura;-e-mail memorizzata potenzialmente su
client e-mail server non sicuri);-perditÃ di integritÃ , corpo del messaggio puÃ² essere modificato in transito oppure modificato dal mail
server;-mancanza di autenticazione,nessuna garanzia sul fatto che la mail provenga da che Ã¨ indicato nel campo from;
****

8. Descrivere la modalit`a di tunnel del protocollo IPSec.
viene criptato l'intero pacchetto IP, non rivelando, al di fuori del tunnel, indirizzi IP e porte usate da sorgente e destinazione. In questa
modalitÃ si usano collegare fra loro due diverse reti, con i rispettivi client inconsapevoli della presenza di un tunnel.
****

1. Dire cosa si intende per virus polimorfo e quali sono le caratteristiche delle signature di tale tipologia di virus.
Ã¨ un virus in grado di modificarsi, assume un grande numero di forme. Deve cambiare casualmente i dati che lo compongono.Deve riposizionare in modo
casuale le parti che lo compongono.Inoltre difficile da riconoscere perche cambia ad ogni infezione la propria signature.
****

2. Dire cosa si intende per virus transiente, virus residente e virus polimorfico.
Transiente: quando la vita del virus dipende da quella del programma che lo ospita. Residente quando il virus Ã¨ in memoria e rimane attivo e puÃ²
essere attivato come un programma stand-alone. Polimorfo (vedi sopra)
****

8. Descrivere a cosa servono i numeri di sequenza del protocollo IPSec.
Una successione di numeri monotonicamente crescente, che identifica il pacchetto all'interno delle Security Association e previene da replay-attack.
****

X) DIFFERENZA TRA WORM E RABBIT
worm:propaga copie di se stesso attraverso la rete al fine di saturare le reti di trasmissione.Rabbit:replica se stesso con lo scopo di saturare le
risorse del sistema.
****

X)Cosa sono gli IDS e le loro CARATTERISTICHE.
Gli ids non si sostituiscono ai normali controlli, ma cerca di scoprire i loro fallimenti. Chi entra in un sistema abusivamente compie operazioni che
un utente normale non fa. Attacchi sono di solito associati ad una violazione del controllo dell'accesso che di norma viene rilevato dall'ids.Le
caratteristiche degli ids sono: Devono poter essere eseguiti senza la supervisione degli utenti.Non deve essere una scatola nera.Deve essere
resistente ai guasti, agli attacchi, deve richiedere un minimo di overhead, deve essere adattabile al sistema in osservazione.Deve far fronte a
cambiamenti nel comportamento del sistema.
****

3. Descrivere a cosa servono i sistemi di intrusion detection e quali sono le differenze tra i sistemi host-based e networkbased.
GLI IDS SONO (vedi sopra). Host based, operano su una singola macchina. Network based controllano tutto il traffico di rete.
****

7. Descrivere le caratteristiche dei sistemi per il controllo delle intrusioni di tipo anomaly detection. Si richiede inoltre di descrivere cosa rappresentano i profili e di descrivere i problemi legati alla definizione di tali profili.
Anomaly detection assume che tutte le attivitÃ intrusive siano anomale, basate sulla definizione di profili che descrivano il normale
funzionamento.Segnala deviazioni dai profil.Capace di riconoscere nuovi attacchi.I profili rappresentano:attivitÃ di login e sessione,esecuzione di
comandi e programmi, attivitÃ di accesso al firewall r/w/x.Problemi:scelta delle metriche,scelta dei threadshold(doglia d'allarme) e delle funzioni
per evitare falsi positivi e negativi;scelta dei modelli di base.Segnalazione di tipo statico che va interpretata da un esperto umano.
****
8. Nellâ€™ambito del protocollo SSL, dire a cosa serve il protocollo authentication header specificando, in particolare, i tipi di attacchi che previene insieme con una loro descrizione.
l'SSL Ã¨ una suite protocollare che fornisce servizi di sicurezza ad applicazioni che usano canali di comunicazione in stream. Utilizza sia
crittografia simmetrica che asimmetrica.L'authentication header fornisce supporto per l'integritÃ dei dati e di autenticazione dei pacchetti
IP.ATTACCHI:man in the middle,male randomizzazzione della chiave crittografica.
****
9. Nellâ€™ambito del servizio di autenticazione Kerberos, descrivere le tre fasi che lo caratterizzano.
Kerberos ha tre obbiettivi: autenticazione:verifica di identitÃ di un client o di un servizio.autorizzazione:autorizza un client autenticato ad
utilizzare un particolare servizio.accounting:verifica la quantitÃ di risorse utilizzate da un particolare client.
****
6. ACL e capability: cosa rappresentano? Illustrare i vantaggi e gli svantaggi.
Con il termine capability si intende in informatica un meccanismo di protezione delle risorse orientato agli oggetti complementare alle ACL.
I sistemi che utilizzano le capability associano a ciascun processo una lista di capability (o C-list), che descrive per l'appunto a quali oggetti
(per esempio file) il processo puÃ² accedere. Una C-list puÃ² essere formata da dei nodi, ciascuno dei quali rappresenta i permessi su un determinato
oggetto puntato.Esempi:in hardware: ad ogni parola in memoria viene aggiunto uno speciale tag che indica se la parola contiene una capability. Solo
il sistema operativo possiede i requisiti per poter modificare questi tag.In spazio-kernel: il sistema operativo ordina a ciascun processo che tenta
di accedere ad un determinato oggetto di verificarne dapprima i permessi consultando una C-list.In spazio-utente: le C-list sono memorizzate in
spazio-utente, ma per questo motivo devono venire crittografate per impedire contraffazioni da parte degli utenti.
****