COMPUTER SECURITY

Definizione: la protezione offerta ad un sistema di informazione automatizzato al fine di raggiungere gli obiettivi di preservare l'integrità, la disponibilità e la riservatezza delle risorse del sistema (comprende hw, sw, firmware, informazioni/dati e telecomunicazioni).

Obiettivi chiave della Computer Security:

- Riservatezza: la riservatezza dei dati assicura che le informazioni private o riservate non siano rese disponibili o divulgate a persone non autorizzate. La privacy garantisce che le persone controllino o influenzino a chi e da chi le proprie informazioni possano essere divulgate.
- Integrità: l'integrità dei dati assicura che le informazioni e i programmi siano modificati sono in un modo specificato e autorizzato. L'integrità del sistema assicura che un sistema esegua la funzione prevista in modo inalterato, libera da manipolazioni non autorizzate deliberate o involontarie del sistema.
- Disponibilità: assicura che i sistemi funzionino rapidamente e il servizio non sia negato agli utenti autorizzati.

NB:

- Una perdita di riservatezza è la divulgazione non autorizzata di informazioni.
- Una perdita di integrità è la modifica o la distruzione non autorizzata di informazioni.
- Una perdita di disponibilità è l'interruzione dell'accesso ad un sistema di informazione.

Altri due concetti importanti:

- Autenticità: la proprietà di essere un vero gruppo che può essere verificato e considerato affidabile, ossia la fiducia nella validità di una connessione, di un messaggio, di un mittente. Verificare che gli utenti siano chi dicono di essere e che ogni input in arrivo al sistema provenga da una fonte attendibile.
- Responsabilità: l'obiettivo di sicurezza che genera il requisito di assegnare univocamente delle azioni all'entità che le compie. Dobbiamo essere in grado di scovare una violazione della sicurezza. I sistemi devono tenere un registro delle proprie attività per consentire alle successive anali di tracciare le violazioni di sicurezza o aiutare nelle controversie sulle transazioni.

Tabella di vari attacchi e conseguenze.

Conseguenza : Divulgazione non autorizzata, una circostanza in cui un'entità ottiene l'accesso a dati per i quali non è autorizzata.

Attacchi:

- Esposizione: i dati sensibili vengono rilasciati direttamente a un'entità non autorizzata
- Intercettazione: un'entità non autorizzata accede direttamente a dati sensibili, attraverso fonti e destinazioni autorizzate.
- Inferenza: un attacco dovuto al fatto che un'entità non autorizzata accede indirettamente a dati sensibili sfruttando le caratteristiche o i mezzi di comunicazione. (Non necessariamente a dati contenuti nella comunicazione).
- Intrusione: un'entità non autorizzata ottiene l'accesso a dati sensibili eludendo la protezione di sicurezza di un sistema.

Conseguenza: Inganno, ossia una circostanza in cui un'entità autorizzata ottiene dati falsi ritenendoli veritieri.

Attacchi:

- Mascheramento: un'entità non autorizzata accede a un sistema o esegue un atto dannoso presentandosi come un'entità autorizzata.
- Falsificazione: dati falsi ingannano un'entità autorizzata.
- Ripudio: un'entità inganna un'altra negando falsamente la responsabilità di un atto.

Conseguenza: Rottura, una circostanza o evento che interrompe o impedisce il corretto funzionamento dei servizi e delle funzioni di sistema.

Attacchi:

- Incapacitazione (non esiste in italiano -> Incapacitation): impedisce o interrompe il funzionamento del sistema disabilitando un componente dello stesso.
- Corruzione: altera in modo indesiderato il funzionamento del sistema modificando negativamente funzioni o dati del sistema.
- Ostruzione: un attacco che interrompe la fornitura dei servizi di sistema ostacolando il funzionamento dello stesso.

Conseguenza: Usurpazione, un evento che determina il controllo di servizi o funzioni di sistema da parte di un'entità non autorizzata.

Attacchi:

- Appropriazione indebita: un'entità si assume il controllo logico o fisico non autorizzato di una risorsa di sistema.
- Uso improprio: fa si che un componente del sistema esegua una funzione o un servizio che è dannoso per la sicurezza dello stesso.

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

ATTACCHI PASSIVI
Si tenta di apprendere o utilizzare le informazioni dal sistema ma non si influisce sulle risorse dello stesso.
Rientrano tra questi le intercettazioni e il monitoraggio di trasmissioni.
L'obiettivo è ottenere informazioni dai dati trasmessi.
Difficile da rilevare poiché non lasciano traccia di modifiche su dati e risorse.
Per impedire questi attacchi si fa ricorso alla crittografia.
Si tratta quindi di un approccio di prevenzione più che di individuazione.

ATTACCHI ATTIVI
Si tratta di modificare flussi di dati o crearne di falsi.
Quattro categorie:

- Riproduzione: implica la cattura passiva di un'unità di dati e la sua successiva ritrasmissione per produrre un effetto non autorizzato.
- Mascheramento: ha luogo quando un entità finge di esserne un'altra.
- Modifica dei messaggi: una parte di un messaggio legittimo viene alterata, oppure viene alterata la sequenza di invio dei messaggi o anche ritardato l'invio.
- Negazione di servizio: impedisce o inibisce il normale utilizzo o la gestione delle strutture di comunicazione, ad esempio si interrompe un'intera parte di rete.

MODELLI DI COMPORAMENTO DELL'INTRUSO
Hackers:

- Tradizionalmente coloro che lo fanno lo fanno per il brivido dell'azione.
- Gli attaccanti spesso cercano obiettivi di opportunità e quindi condividono informazioni con gli altri.
- Gli intrusi benigni consumano risorse e possono rallentare le prestazione per gli utenti legittimi.
- I sistemi di rilevamento delle intrusioni e i sistemi di prevenzione delle intrusioni sono progettati per contrastare questo tipo di minaccia da parte di hacker.
- I team di risposta alle emergenze informatiche sono iniziative cooperative che raccolgono informazioni sulle vulnerabilità del sistema e condividono ciò che scoprono con i responsabili del sistema (sgamano falle a pagamento).

1. Select the target using IP lookup tools such as NSLookup, Dig, and others.
2. Map network for accessible services using tools such as NMAP.
3. Identify potentially vulnerable services (in this case, pcAnywhere).
4. Brute force (guess) pcAnywhere password.
5. Install remote administration tool called DameWare.
6. Wait for administrator to log on and capture his password.
7. Use that password to access remainder of network.

Società criminali:

- Gruppo organizzato di hackers.
- Si organizzano e scambiano consigli in forum nascosti.
- Un obiettivo comune sono file riguardanti carte di credito nei server degli e-commerce.
- Di solito hanno obiettivi specifici, o almeno classi di obiettivi, in mente.
- Attacchi rapidi e veloci.

1. Act quickly and precisely to make their activities harder to detect.
2. Exploit perimeter through vulnerable ports.
3. Use Trojan horses (hidden software) to leave backdoors for reentry.
4. Use sniffers to capture passwords.
5. Do not stick around until noticed.
6. Make few or no mistakes.

Attaccanti interni:

- Tra i più difficili da individuare e prevenire.
- Può essere motivato dalla vendetta o semplicemente pensa di avere il diritto di farlo.
- I dipendenti hanno già accesso e conoscenza della struttura e del contenuto dei database aziendali.

1. Create network accounts for themselves and their friends.
2. Access accounts and applications they wouldn't normally use for their daily jobs.
3. E-mail former and prospective employers.
4. Conduct furtive instant-messaging chats.
5. Visit Web sites that cater to disgruntled employees, such as f'dcompany.com.
6. Perform large downloads and file copying.
7. Access the network during off hours.

MALWARE

Termine generale per indicare un software dannoso.

Software ideato per causare danni o consumare risorse di un computer designato.

Spesso nascosto o mascherato come software legittimo.

In alcuni casi si diffonde ad altri computer tramite e-mail o dispositivi infetti.

Backdoor:

- Anche conosciuto come trapdoor.
- Un punto di accesso segreto in un programma che consente di accedere senza eseguire le consuete procedure di accesso di sicurezza.
- Un hook (aggrappo) di manutenzione è una backdoor che i programmatori usano per debuggare e testare programmi che richiedono una lunga configurazione.
- Diventa una minaccia quando la si usa per ottenere un accesso non autorizzato.
- E' difficile implementare i controlli del sistema operativo per le backdoor.

Logic Bomb:

- Uno dei più vecchi tipi di attacco.
- Codice incorporato in un programma legittimo pronto ad "esplodere" quando vengono soddisfatte determinate condizioni.
- Una volta innescata una bomba può alterare o cancellare dati o interi file, causare un arresto della macchina o fare altri danni.

Trojan Horse:

- Programma utile o apparentemente utile che contiene codice nascosto che, quando invocato, esegue alcune funzioni indesiderate e dannose.
- I Trojan Horse si adattano a uno di questi tre modelli:
    1. Continuano a svolgere la funzione del programma originale e contemporaneamente un'attività malevola.
    2. Continuano a svolgere la funzione del programma originale ma modificandone il funzionamento per eseguire l'attività malevola.
    3. Esecuzione diretta dell'attività malevola.

Platform Independent Code:

- A volte indicato come codice mobile.
- Programmi che possono essere spediti invariati a un insieme vasto di piattaforme ed eseguiti con semantica identica.

- Trasmesso da un sistema remoto a un sistema locale e quindi eseguito su quest'ultimo senza la volontà esplicita dell'utente.
- Spesso si comporta come un meccanismo per virus, un worm o un trojan horse da trasmettere all'utente.
- Sfrutta i vantaggi delle vulnerabilità.

Multiple-Threat Malware:
- Infetta in più modi.
- Un virus multipartito è in grado di infettare più tipi di file.
- Un attacco combinato utilizza più metodi di infezione o trasmissione per massimizzare la velocità del contagio e la gravità dell'attacco.
- Un esempio di questo tipo di approccio combinato è Stuxnet.

Virus:
- Software che infetta altri programmi modificandoli:
    - Porta con se codice per auto duplicarsi.
    - Viene incorporato in un programma su un computer
    - Quando il computer infetto entra in contatto con un pezzo di software non infetto, una copia del virus passa nel programma.
    - L'infezione può essere diffusa scambiando dischi da computer a computer o attraverso una rete.
- Un virus informatico ha tre parti:
    - Un meccanismo di infezione
    - Un attivatore
    - Un payload
        - Può comportare danni
        - O attività benigne ma evidenti
- Fasi del virus:
    - Fase dormiente:
        - Il virus è inattivo
        - Sarà eventualmente attivato da qualche evento.
        - Non tutti i virus hanno questa fase
    - Fase di propagazione
        - Il virus inserisce una copia identica di se stesso in altri programmi o in certe aree del disco di sistema
    - Fase di attivazione
        - Il virus viene attivato per eseguire la funzione per la quale è stato progettato
        - La fase di attivazione può essere causata da una varietà di eventi di sistema
    - Fase di esecuzione
        - La funzione viene eseguita
        - La funzione potrebbe essere innocua (messaggio sullo schermo) o dannosa (distruzione di programmi e file di dati)
- Classificazione dei virus:
    - Non esiste uno schema di classificazione universalmente accettato
    - La classificazione per target include le seguenti categorie:
        - Boot sector infector ossia infetta un record di avvio principale e si diffonde quando un sistema viene avviato dal disco contenente il virus
        - File infector ossia infetta i file che l'OS o la shell considerano eseguibili
        - Macro Virus ossia infetta file con codice macro interpretato da un'applciazione

- Strategia di occultamento:
    - Una classificazione dei virus mediante la strategia di occultamento:
        - Virus crittografato ossia una chiave di crittografia casuale crittografa il virus
        - Virus furbo ossia si nasconde dal rilevamento dell'antivirus
        - Virus polimorfo ossia muta con ogni infezione. Le copie sono funzionalmente equivalenti ma hanno pattern di bit totalmente differenti.
        - Virus metamorfo ossia mutua con ogni infezione. Si riscrive completamente dopo ogni iterazione.

Macro Virus:

- A metà degli anni '90 i Macro Virus sono diventati i virus più diffusi
- Sono particolarmente minacciosi perché:
    - Sono indipendenti dalla piattaforma. Molti Macro Virus infettano documenti Word o altri documenti Office.
    - Infettano documenti, non porzioni di codici eseguibili
    - Sono facilmente diffondibili, metodo comune è via e-mail
    - I controlli di accesso al file system sono di uso limitato per impedirne la diffusione.

E-Mail Virus:

- I primi e-mail virus in rapida diffusione utilizzavano una macro di Microsoft Word incorporata in un allegato:
    - Se il destinatario apre l'allegato, la macro è attivata.
    - Il virus e-mail si inoltra a tutti gli utenti nella lista contatti del primo destinatario.
    - Il virus fa danni locali al sistema dell'utente.
- Nel 1999 il virus venne potenziato:
    - Può essere attivato soltanto aprendo una mail e non aprendo per forza l'allegato.
    - Il virus utilizza il linguaggio di scripting Visual Basic supportato dal pacchetto e-mail.

Worms:

- Un programma in grado di replicarsi e inviare copie da un computer all'altro attraverso la connessione di rete.
- Alla ricezione di un worm può essere attivato per replicarsi e propagarsi di nuovo.
- Oltre alla propagazione, il worm di solito svolge alcune funzione indesiderate.
- Cerca attivamente macchine da infettare e in ognuna di questa infettata funge da trampolino di lancio automatico per attacchi ad altre macchine.
- Per replicarsi e propagarsi utilizza mezzi di network:
    - Struttura mail elettronica: invia una copia di se stesso ad altri sistemi in modo che il suo codice venga eseguito quando l'e-mail o l'allegato viene ricevuto e visualizzato.
    - Funzionalità di esecuzione remota: esegue una copia di se stesso su un altro sistema usando una funzione di esecuzione remota esplicita o sfruttando un difetto di programma in un servizio di rete per sovvertire le sue operazioni.
    - Funzionalità di accesso remoto: accede a un sistema remoto come utente e quindi utilizza i comandi di quest'ultimo per copiare se stesso da un sistema all'altro.

Bots:

- Un programma che acquisisce segretamente il controllo su un computer collegato a internet e quindi utilizza tale computer per lanciare attacchi difficili da collegare al creatore del bot. Anche conosciuto come Zombie o Drone.
- Generalmente installato su tantissimi computer appartenenti a terze parti ignare.
- Una collezione di Bot che agiscono in maniera coordinata si chiama BOTNET

- Un Botnet ha tre caratteristiche:
    - La funzionalità di un bot
    - Controllato da remoto
    - Un metodo di propagazione dei bot per costruire il botnet
- Usi:
    - DDoS attack (Distributed denial-of-service) che blocca dei servizi all'utente
    - Spamming che invia messaggi in maniera massiva con una serie di mail
    - Sniffing traffic per ottenere informazioni sensibili come username o password
    - Spreading new malware ossia per diffondere malware
    - Manipulating online polls/games possibile poiché ogni bot ha un distinto IP e appare come una persona normale
    - E tanti aaaaltri

Remote Control Facility:

- Si deve distinguere un bot da un worm: un worm si propaga e si attiva, mentre un bot è controllato da una struttura centrale.
- Un mezzo tipico per implementare un Remote Control Facility è un server IRC: tutti i bot si uniscono ad un canale specifico su questo server e trattano i messaggi in arrivo come comandi.
- Le botnet più recenti tendono a utilizzare canali di comunicazioni nascosti tramite protocolli come HTTP.
- Meccanismi di controllo distribuiti vengono anche utilizzati per evitare un singolo punto di errore.

Constructing the attack network:

- Il primo passo in un attacco botner da parte di un attaccante è di infettare un certo numero di macchine con i bot che verranno utilizzati per portare a termine l'attacco.
- Ingredienti essenziali:
    - Software che sia in grado di eseguire l'attacco
    - Una vulnerabilità in un ampio numero di sistei
    - Una strategia di localizzazione di macchine vulnerabili (un proccesso chiamato scanning)
- Nello scanning process l'attaccante deve per primo cercare macchine vulnerabili e infettarle.
- Il software del bot ripete nelle macchine infette lo stesso processo di scanning finchè un'ampia rete di macchine infette non è stata creata.

Rootkit:

- Insieme di programmi installati su un sistema per mantenere l'accesso di amministratore (root) a quel sistema.
- L'accesso root consente l'accesso a tutte le funzioni e i servizi del sistema operativo.
- Il rootkit modifica le funzionalità standard dell'host in modo malevolo e furtivo. Con l'accesso root un utente malintenzionato ha il controllo totale del sistema e può aggiungere, eliminare, modificare file, monitorare processi, lavorare attraverso rete e ottenere anche l'accesso backdoor.
- Un rootkit si nasconde sovvertendo i meccanismi che controllano e segnalano i processi, i file, i registri su un pc.
- Classificazione in base a come sopravvivono dopo il riavvio o alla modalità d'esecuzione:
    - Persistente: attivato ogni volta che il sistema si avvia.
    - Memory based: non ha codice persistente e non può sopravvivere a un riavvio.
    - User-mode: intercetta le chiamate alle API e modifica i risultati restituiti.
    - Kernel-mode: può intercettare le chiamate alle API native in modalità kernel. Può nascondere la presenza di unu processo malware rimuovendolo dall'elenco dei processi attivi dal kernel.

- Installazione:
    - I rootkit non si affidano direttamente a vulnerabilità per accede a un computer.
    - Un metodo di installazione è attravero un Trojan Horse.
    - Un altro mezzo di installazione può avvenire da parte di un hacker.

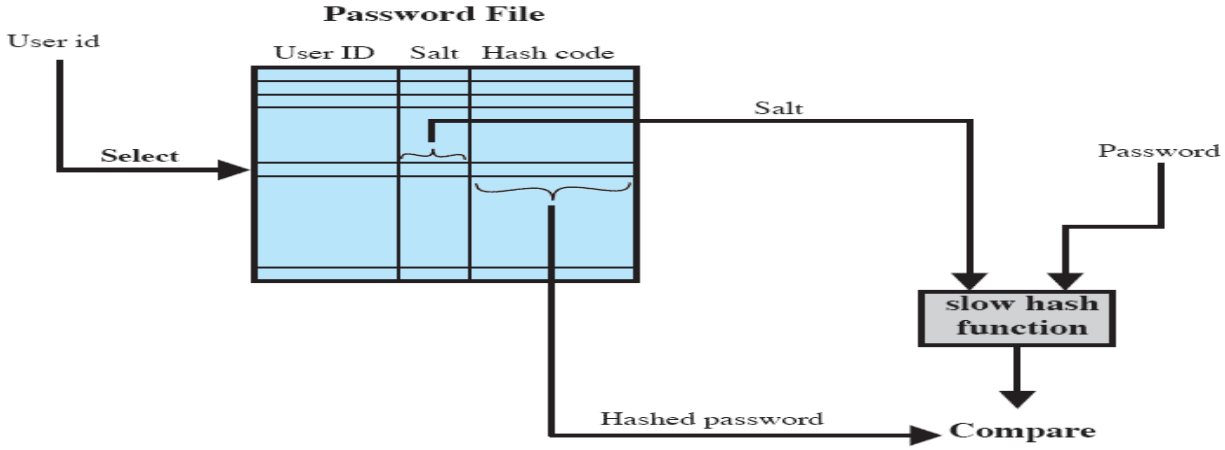
Attacchi con syscall:

- I programmi operativi a livello utente interagiscono con il kernel tramite syscall.
- In linux a ciascuna syscall viene assegnato un numero univoco.
- Tre tecniche possono essere utilizzate per modifica le chiamate di sistema:
    - Si può modificare la tabella delle chiamate di sistema in modo che punti al codice della rootkit.
    - Si può modificare gli obiettivi della tabella delle syscall.
    - Reindirizzare l'intera tabella delle syscall.

OPERATING SYSTEM DEFENSE

Autenticazione basata su password:

- Un metodo di difesa ampiamente utilizzato contro gli intrusi è il sistema delle password.
- La password serve pe autenticare l'ID del singolo accesso al sistema.
- L'ID fornisce sicurezza attraverso:
    - Determinando se l'utente è autorizzato ad ottenere l'accesso al sistema.
    - Determinando i privilegi d'accesso in funzione dell'utente.
    - Controllo d'accesso discrezionale.



(b) Verifying a password

- Il sale serve a tre cose:
    - Impedisce che password duplicate siano visibili nel file di password. (Anche se due utenti scelgono la stessa password verranno assegnati a valore di sale diversi).
    - Aumenta notevolmente la difficoltà di attacchi dizionario.
    - Diventa quasi impossibile scoprire se una persona ha utilizzato la stessa password su piu sistemi d'accesso.

Schema Password UNIX:

- Esistono due minacce per questo schema:
    - Un utente può guadagnare un account ospite su una macchina e poi utilizzare un programma cracker (un programma che indovina la password) sul sistema.

    - Se l'attaccante è in grado di ottenere una copia del file delle password, il cracke program può essere utilizzato su un'altra macchina. Questo permette di scorrere milioni di password possibili in un tempo ragionevole.

Autenticazione basata sul Token:

- Gli oggetti che un utente possiede ai fini dell'autenticazione sono chiamati Token.
- Due tipi di token:
    - Memory cards: possono conservare dati ma non processarli. La più comune è la carta di credito con una banda magnetica sul retro. Una banda magnetica può memorizzare solo un semplice codice di sicurezza che può esser letto e riprogrammato da un lettore di schede economico. Ci sono anche schede che includono una memoria elettronica interna. Può essere utilizzata da sola o con qualche forma di password (PIN personal identification number).
    - Smart Cards: include un processore. Un oggetto intelligente che sembra una carta di credito è chiamato smart card. Possono essere calcolatrici, chiavi o altri piccoli oggetti portatili. L'interfaccia prevede una tastiera e un display per l'interazione uomo/token. Comunicano con un lettore specifico per le smart card. L'autenticazione può essere statica, dinamica generando una One Time Password o attraverso delle domande effettuate all'utente.

Autenticazione statica Biometrica:

- Si cerca di autenticare una persona attraverso le proprie uniche caratteristiche fisiche.
- Esempi di caratteristiche fisiche statiche:
    - Impronta digitale
    - Profilo della mano
    - Caratteristiche facciali
    - Scansione retina o iride
- Esempi di caratteristiche dinamiche:
    - Timbro della voce
    - Firma
- Caratteristiche fisiche:
    - Caratteristiche facciali: mezzi più comuni per l'identificazione tra persone. Esempio: occhi, sopracciglia, naso, labbra… Un approccio diverso è quello di usare una camera ad infrarossi per riprodurre una scansione termica facciale.
    - Impronte digitali: modello di creste e solchi sulla superficie del polpastrello. Unica per ogni uomo.
    - Geometria della mano: identifica caratteristiche della mano tra cui la forma la lunghezza e la grossezza delle dita.
    - Scansione retina: modello formato dalle vene sotto la superficie retinica è unico. Una scansione della retina ottiene questo modello attraverso l'uso di infrarossi.
    - Iride: i dettagli dell'iride sono unici.
    - Firma: ognuno di noi ha una scrittura personale.
    - Voce: il modello della voce dipende fortemente dalle caratteristiche fisiche e anatomiche dell'individuo.

Controllo dell'accesso:

- Una politica di controllo degli accessi stabilisce quali tipi di accesso sono consentiti, in quali circostanze e da chi.
- Le politiche d'accesso sono di solito raggruppate in queste categorie:

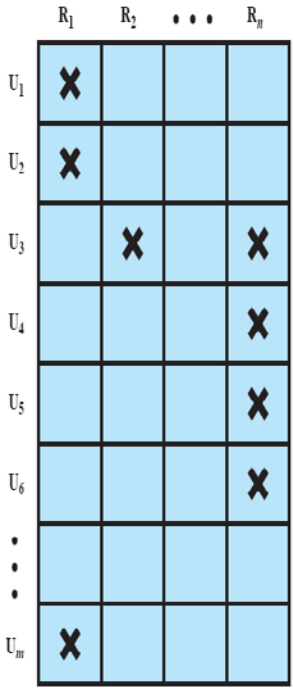
- Controllo d'accesso discrezionale (DAC): controlla l'accesso in base all'identità del richiedente e alle regole di accesso che indicano quali sono (o non sono) i richiedenti autorizzati.
- Controllo d'accesso vincolato (MAC) la m sta per Mandatory: controlla l'accesso basandosi sul tipo di utente di cui vengono controllati i permessi d'accesso da un sistema.
- Controllo d'accesso basato sul ruolo (RBAC): controlla l'accesso in base al ruolo di ogni utente e alle regole che indicano quali privilegi ha ogni utente in base al ruolo ricoperto.

		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* - copy flag set

Figure 15.4 Extended Access Control Matrix

Questa è una tabella dei permessi per il primo tipo di controllo. Vieni dapprima identificato in un Subject a cui corrispondo permessi particolari su oggetti.
Il secondo invece dato il tipo di utente, il kernel decide, in base alla richiesta effettuata se tu sei autorizzato ad eseguire tale richiesta. Per il terzo tipo di controllo invece non si fa distinzione tra utenti bensi tra i ruoli che essi ricoprono. Il ruolo è inteso come un lavoro specifico che ogni utente fa. A ogni utente è assegnato un ruolo. A ogni ruolo dei permessi.



		OBJECTS								
		R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
ROLES	R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	R_2		control		write *	execute			owner	seek *
	. . .									
	R_n			control		write	stop			

SISTEMA DI RILEVAMENTO INTRUSIONE BASATO SULL'HOST (IDS)
Monitora l'attività sul sistema in vari modi per rilevare comportamenti sospetti. Lo scopo principale è rilevare intrusioni, registrare eventi sospetti e inviare allarmi. Può rilevare sia intrusioni interne che esterne.
Rilevamenti anomali:

- Raccolta di dati relativi al comportamento degli utenti autorizzati nel tempo.
- Rilevamento soglia.
- Rilevamento basato sul profilo.

Rilevamento firma:

- Definisce un insieme di regole o di modelli di attacco che possono essere utilizzati per decidere se un dato comportamento è quello di un intruso.

Alcune informazioni sull'attività dell'utente vengono fornite in tempo reale all'IDS.
Se il sistema di controllo è nativo è comodo perché non abbiamo bisogno di software aggiuntivi per raccogliere i dati che ci interessa però purtroppo i registri di controllo nativi potrebbero non contenere le informazioni necessarie o in parte per scovare un'intrusione.
Se invece ci affidiamo ad un software specifico, ne usufruiamo grazie ad un venditore, potremmo comodamente trasferirlo su tantissimi sistemi. Lo svantaggio ovviamente è l'overhead che si crea nel momento in cui si devono fornire dati al software.

ANTIVIRUS APPROCHES
La soluzione ideale per minacce virus è la prevenzione. L'obiettivo di evitare infezioni sul proprio sistema non è del tutto raggiungibile, comunque sia la tattica della prevenzione riduce decisamente il numero di attacchi virali con successo. Se il rilevamento ha esito positivo, ma l'identificazione o la rimozione non è possibile, l'alternativa è scartare il programma infetto e ricaricare una versione pulita da una copia di backup.
Fasi:

- Rilevamento: una volta che l'infezione è avvenuta, l'antivirus determina l'attività del virus e lo localizza.
- Identificazione: una volta localizzato si cerca di identificarlo confrontandolo con le firme antivirali sopra descritte.
- Rimozione: Una volta identificato si rimuovono tutte le tracce del virus dal programma infetto e lo si ripristina allo stato originale. L'obiettivo è di rimuoverlo da tutti i sistemi affinché non si possa più diffondere.

GENERIC DECRYPTION (GD)
Consente al programma antivirus di rilevare facilmente anche i virus polimorfi più complessi mantenendo allo stesso tempo una velocità di scansione elevata. Quando viene eseguito un file contenente un virus polimorfo, quest'ultimo deve decrittografarsi per attivarsi. Di conseguenza all'apertura di questi file eseguibili viene effettuata una scansione tramite uno scanner GD.
Il problema di progettazione più complesso con uno scanner GD è determinare il tempo di esecuzione di ogni interpretazione.
Un GD scanner contiene:

- Un modulo di controllo di emulazione: controlla l'esecuzione del codice in analisi.
- Scanner delle firme antivirali: un modulo che analizza il codice in cerca di virus.
- Emulatore della CPU: un computer virtuale basato su software. I file eseguibili vengono interpretati dall'emulatore in modo che il processore sottostante non venga intaccato.

DIGITAL IMMUNE SYSTEM

Un approccio completo alla protezione dai virus sviluppato da IBM e perfezionato da Symantec. La necessità dello sviluppo nasce dalla sempre più alta presenza di virus che si propaga via internet.

Due tendenze in internet hanno avuto un impatto sempre crescente sul tasso di propagazione dei virus negli ultimi anni:

- Sistemi di posta integrati.
- Sistemi di programmi mobili (ossia, spostamento di codice malevolo su più piattaforme).

L'obiettivo del sistema è quello di fornire tempi di risposta rapidi in modo che i virus possano essere eliminati nel migliore dei casi appena vengono introdotti nei sistemi.

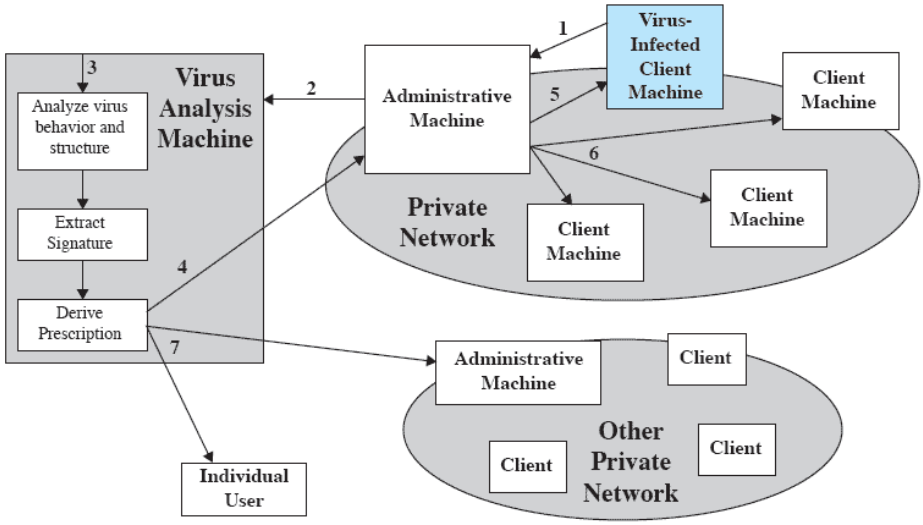


Figure 15.9 Digital Immune System

Appena un client viene infettato e l'analisi da esito positivo si notificano tutte le altre macchini amministratrici che diffonderanno l'avviso ai loro rispettivi client.

BEHAVIOR BLOCKING SOFTWARE

Si integra con il sistema operativo e monitora il comportamento del programma in tempo reale per scovare azioni dannose.

Potrebbe includere:

- Aprire o modificare determinati file.
- Formattazione dischi.
- Modifiche ai file eseguibili o macro.
- Modifica delle impostazioni di sistema critiche.
- Comunicazione network.

Operazioni:

1. L'amministratore setta politiche sui comportamenti accettabili del software e le carica su un server o sui desktop.
2. Il software dannoso riesce a superare il firewall.
3. Il software behavior-blocking segnala il codice sospetto al server e "insabbia" il software sospetto per impedirgli di avviarsi.
4. Il server avvisa l'amministratore che il codice sospetto è stato identificato e messo in quarantena e resta in attesa della decisione dell'amministratore sulla volontà di quest'ultimo di rimuoverlo o di autorizzarne l'esecuzione.

CONTROMISURE AI WORM

Una volta che il worm infetta una macchina è possibile rilevarlo con un software antivirus. La sua propagazione genera una considerevole attività di rete, quindi l'attività e il monitoraggio dell'utilizzo di quest'ultima possono essere un'arma di difesa.

Classi di difesa contro i worm:

A. Scansione worm basata sul filtro della firma virale: genera una firma del worm che viene poi utilizzata per impedire che le scansioni di worm entrino/escano da una rete/host.
B. Filtraggio dei worm in base al loro contenuto: simile alla classe A, ma si concentra sul contenuto del worm piuttosto che sulla firma.
C. Blocco del worm basato sulla classificazione del payload: le tecniche di rete esaminano i pacchetti per vedere se contengono worm.
D. Scansione di rilevamento del Threshold random walk (TRW): sfrutta la casualità nella scelta delle destinazioni da connettere come un modo per rilevare se uno scanner è in funzione.
E. Limitazione del rate: limita la velocità del traffico da un host infetto.
F. Blocco del rate: blocca immediatamente il traffico in uscita quando viene superata una soglia in termini di velocità di connessione.

CONTROMISURE AI BOT

Gli IDS e i Digital Immune System sono utili contro i bot. Una volta che i bot sono attivati e un attacco è in corso, queste contromisure possono essere utilizzate per rilevare l'attacco.

L'obiettivo principale è cercare di rilevare e disabilitare la botnet durante la sua fase di costruzione.

CONTROMISURE AI ROOTKIT

Può essere difficile da individuare e neutralizzare. Molti degli strumenti amministrativi possono essere compromessi e resi inutilizzabili. Per contrastarli si necessità di una varietà di strumenti di sicurezza a livello di rete e computer. I sistemi di rilevamento delle intrusioni basati sulla rete e su host possono cercare le firme di codice degli attacchi noti di rootkit nel traffico d'entrata. Anche il software antivirus può rilevare le firme conosciute del rootkit.