Hello I’m Ostap

About
I am a Software Architect/Lead Developer consultant, focused on Cyber Security and Web3 Enthusiast.

I ❤️ sustainable coding 🌍.

Currently:
- Co-founder of wesync.dev
- Technical Instructor
- Consulting at Sky and several startups as software architect/developer
- Working on a web3 social app

linkedin *linkedin.com/in/ostap-markin-505441173/*
email *ostap.m@pm.me*

Programma del corso

- Introduzione al problema della sicurezza informatica: da chi, da cosa e come proteggersi.
- Alcune tipologie di minacce note
- Controllo degli accessi
- Sicurezza dei sistemi Web (principali attacchi e attacchi sofisticati) OWASP 10 ed altri
- Secure Programming
- Secure Software Development Lifecycle
- Threat Modelling
- Tanta pratica

Sicurezza informatica

La sicurezza informatica non è ...

... non è crittografia
Crittografia scienza esatta come branca della matematica
• Impossibile violare RSA in tempo polinomiale

Sicurezza scienza inesatta perchè basata su persone e macchine
• Acquisto on-line potenzialmente insicuro

Sicurezza informatica

… non è password

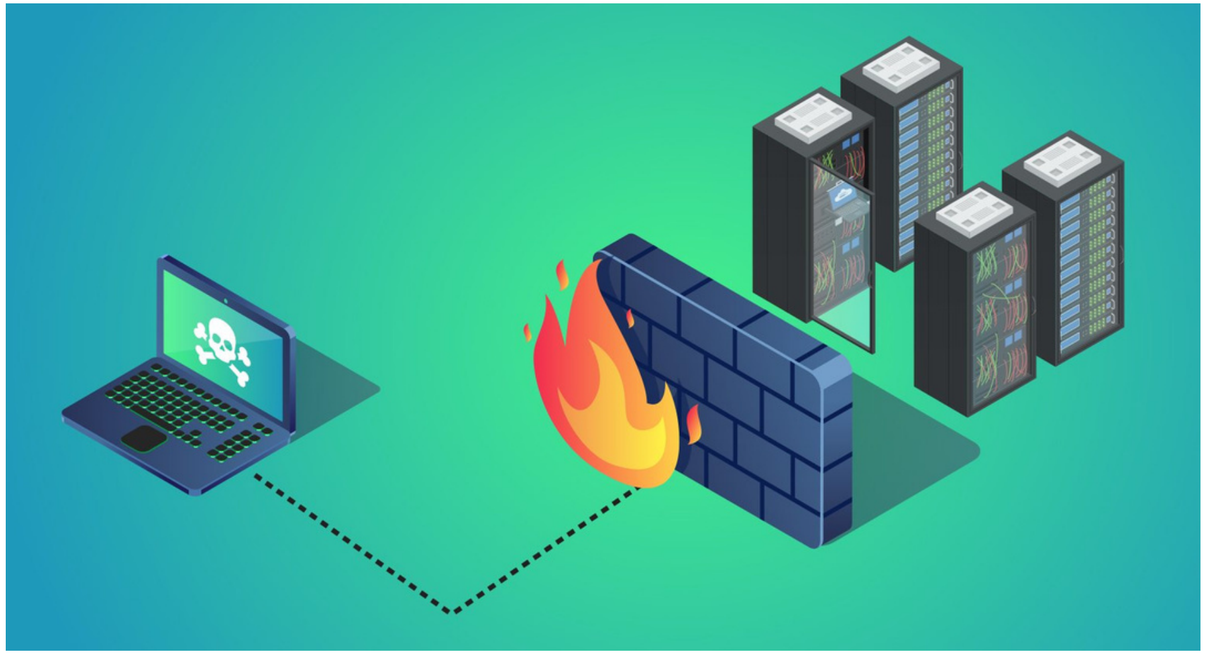
Sistema molto debole!
La password più diffusa è **love**

- Attacchi dizionario
- Attacchi a forza bruta
- Ottenere l’accesso al file delle password

Problemi:
- Come scegliere una buona password?
- Come ricordare una buona password?
- Usare una password per sempre?

Sicurezza informatica

... non è firewall



Sicurezza informatica

la sicurezza è un processo, non un prodotto, una catena la cui resistenza è determinata dall’anello più debole.

La sicurezza informatica (in inglese computer security), è l'insieme dei mezzi, delle tecnologie e delle procedure tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici.

Wikipedia

Sicurezza informatica

- E’ una proprietà di vari livelli architetturali (SO, rete, applicativo, …)
- È costosa nel senso di risorse computazionali, gestione, mentalità e utilizzo
- Rimane un campo aperto anche per i colossi dell’informatica
- *Richiederebbe spesso il ridisegno di un sistema preesistente, il che non è sempre possibile*

Sicurezza informatica

Cyber Security è la disciplina che si occupa della protezione delle informazioni digitali e dei sistemi informatici da attacchi informatici. La Cyber Security si concentra in particolare sulla protezione delle reti, dei dati e dei sistemi da minacce provenienti da Internet.

IT Security è un termine spesso usato come sinonimo di Cyber Security, ma in realtà c'è una sottile differenza tra i due. L'IT Security si occupa della protezione dei sistemi informatici di un'organizzazione, mentre la Cyber Security si occupa della protezione delle informazioni digitali da minacce informatiche.

ICT Security unisce il mondo fisico a quello logico, si pone come anello di congiunzione tra la IT security e la cyber security.
È la disciplina che si occupa della protezione di tutti i sistemi e delle tecnologie che compongono l'infrastruttura ICT di un'organizzazione, compresi i dispositivi, le reti, i dati e le applicazioni.

Principi ad alto livello

I principi di sicurezza ad alto livello sono un insieme di linee guida generali che possono essere utilizzate per migliorare la sicurezza di un sistema o di un'organizzazione. Questi principi sono spesso utilizzati dai professionisti della sicurezza per guidare lo sviluppo e l'implementazione di misure di sicurezza.

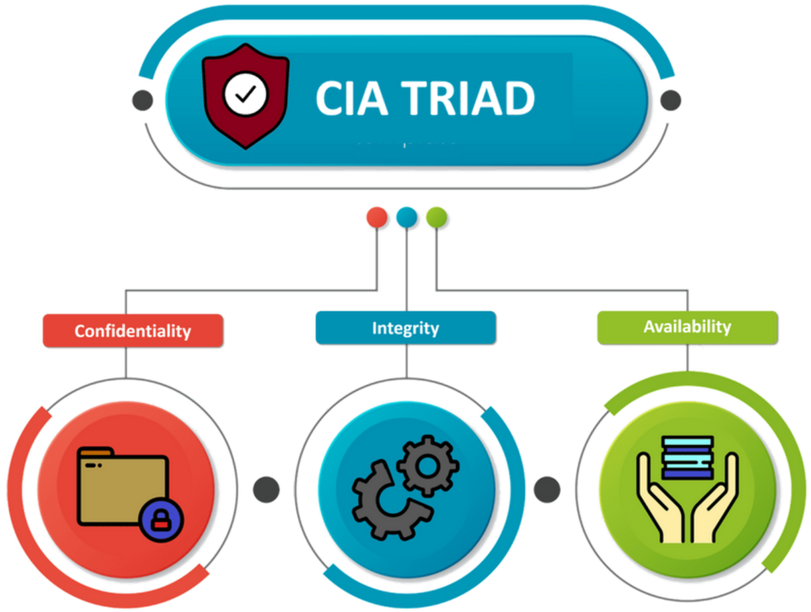
I principi di sicurezza ad alto livello sono spesso suddivisi in tre categorie principali:

- **Principi di sicurezza fisica**: Questi principi si concentrano sulla protezione dei sistemi e dei dati da danni fisici.
- **Principi di sicurezza logica**: Questi principi si concentrano sulla protezione dei sistemi e dei dati da attacchi informatici.
- **Principi di sicurezza procedurale**: Questi principi si concentrano sulla protezione dei sistemi e dei dati attraverso la formazione e le procedure.

I principi di sicurezza ad alto livello sono un punto di partenza importante per la progettazione e l'implementazione di un programma di sicurezza efficace. Questi principi possono aiutare a garantire che i sistemi e i dati siano protetti da una varietà di minacce.

CIA

abilità di proteggere informazioni in base alle nozioni di CIA



Confidentiality

Per confidenzialità dei dati informatici si intende la protezione dei dati durante tutto il loro ciclo di vita.
Ovvero, durante la ***creazione*** di questi ultimi, il loro ***immagazzinamento***, la loro ***trasmissione***, ***diffusione*** e utilizzo da parte di soggetti terzi non autorizzati.

Un'interruzione della confidentiality può avere un impatto significativo sulla reputazione e sull'attività di un'organizzazione. Ad esempio, la divulgazione di informazioni riservate, come informazioni finanziarie o dati personali, può danneggiare la reputazione di un'azienda e portare a sanzioni legali.

Esempi di minacce alla confidentiality:

- **Attacchi informatici**, come malware e attacchi mitm
- **Accesso non autorizzato**, come furti di dati o violazioni di sicurezza
- **Errori umani**

Per garantire la confidentiality:

- **Authentication e Authorization**
- **Crittografia**
- **Controllo degli accessi (Access Control Models)**
- **Formazione degli utenti**

Integrity

Mantenimento dell’incolumità dei dati e la loro salvaguardia. Protezione da ogni tipo di manomissione esterna non autorizzata.
Capacità di mantenere originali i dati e le risorse affinché non vengano in alcun modo modificate o cancellate.

Per garantire la protezione e sicurezza dei dati è necessario attivare delle policy di autenticazione che siano quindi in grado di monitorare gli accessi e i tentativi di accesso.

Esempi di minacce all'Integrity

- Attacchi di **modifica dei dati**: questi attacchi mirano a modificare i dati in modo non autorizzato.
- Attacchi di **inserimento di dati falsi**: questi attacchi mirano a inserire dati falsi in un sistema.
- Attacchi di **distruzione dei dati**: questi attacchi mirano a cancellare o rendere inaccessibili i dati. Possono essere eseguiti utilizzando malware, ransomware o altri attacchi informatici.

Per garantire l'Integrity:

- **Controllo dei dati**
- **Verifica dei dati**
- **Archiviazione dei dati**
- **Formazione degli utenti**

Availability

Availability garantisce che le informazioni siano disponibili per gli utenti autorizzati quando ne hanno bisogno.
Un'interruzione dell'availability può avere un impatto significativo sulle operazioni di un'organizzazione. Ad esempio, un attacco informatico che porta alla perdita di dati può interrompere le attività aziendali, mentre un'interruzione di corrente può impedire agli utenti di accedere ai sistemi informatici.

Esempi di minacce alla disponibilità:

- **Attacchi informatici**, come malware, ransomware e attacchi DDoS
- **Disastri naturali**, come incendi, terremoti e inondazioni
- **Manutenzione o guasti di sistema**
- **Errori umani**

Per garantire la disponibilità delle informazioni:

- **Backup e ripristino dei dati**
- **Distribuzione geografica dei dati**
- **Resilienza dei sistemi informatici**
- **Formazione degli utenti**

Altre proprietà

Non ripudio
Il non ripudio è una proprietà di sicurezza che garantisce che il mittente di un messaggio non possa negare di averlo inviato. Questo è importante per garantire che le transazioni siano valide e che le responsabilità possano essere attribuite alle parti coinvolte.

Esistono diversi modi per implementare il non ripudio. Uno dei modi più comuni è utilizzare la crittografia a chiave pubblica. La crittografia a chiave pubblica consente al mittente di firmare il messaggio utilizzando la sua chiave privata. La firma è un hash del messaggio che è stato crittografato con la chiave privata del mittente. Il destinatario può quindi verificare la firma utilizzando la chiave pubblica del mittente.

Safety
La safety è una proprietà di un sistema che lo protegge da danni irreparabili. Questo è importante per garantire che i dati e le risorse siano protetti da attacchi e abusi.

Esistono diversi modi per implementare la sicurezza. Uno dei modi più comuni è utilizzare la **crittografia**. La crittografia consente di rendere i dati incomprensibili a chiunque non abbia la chiave di decrittazione.
Back-up: Crea copie di backup dei dati e dei sistemi in modo da poterli ripristinare in caso di perdita o danneggiamento.

Attacchi comuni

Complicato isolare i tipi di attacco, in quanto un attaccante sfrutta diversi perimetri (da quelli fisici a quelli digitali).

- *Essere coscienti che per quanto il nostro applicativo ci sembri sicuro, ci sono una serie di vettori d'attacco che sono al di fuori del nostro scope.*

Possiamo distinguire due categorie di attacco

- attacchi tecnologici
- attacchi non tecnologici

Attacchi comuni

categorizzare domini in cui ci sono
le vulnerabilità

- Network
- Malware
- **Web**
- Reversing & Exploiting
- Crittografia

Nuovi trends come *blockchain* e *AI*

https://gandalf.lakera.ai/

Attacchi comuni

Man-in-the-middle (MITM)

Sniffing

Esistono due tipi principali di attacchi **sniffing**:

- **Sniffing passivo**: in questo tipo di attacco, l'attaccante si limita a intercettare i dati che vengono trasmessi in rete. I dati non vengono modificati o alterati in alcun modo.

- **Sniffing attivo**: in questo tipo di attacco, l'attaccante si inserisce nella comunicazione tra due dispositivi e modifica i dati che vengono trasmessi.

Spoofing

Un attaccante si finge un'altra entità. Questo può essere fatto falsificando l'indirizzo IP, l'indirizzo MAC o altri identificatori di un dispositivo.

Esistono diversi tipi di attacchi spoofing, tra cui:

- IP spoofing: l'attaccante falsifica l'indirizzo IP del proprio dispositivo in modo che appaia provenire da un'altra fonte.
- MAC spoofing: l'attaccante falsifica l'indirizzo MAC del proprio dispositivo in modo che appaia provenire da un'altra fonte.
- DNS spoofing: l'attaccante falsifica le risposte DNS in modo da reindirizzare le richieste a un server DNS falso.
- E-mail spoofing: l'attaccante falsifica l'indirizzo e-mail del mittente in modo che un messaggio di posta elettronica appaia provenire da un'altra fonte.

Attacchi comuni

Man-in-the-middle (MITM)

- DNS Spoofing: DNS cache poisoning si verifica quando i record DNS manipolati vengono utilizzati per deviare il traffico online legittimo verso un sito Web falso o spoofato.
- IP Spoofing: simile allo spoofing DNS, ma invece di spoofare il record DNS del sito web, l'attaccante modifica l'indirizzo IP del sito dannoso per farlo apparire come l'indirizzo IP del sito web legittimo.
- SSL Strip: si modificano i certificati SSL di un sito web. L'attaccante può utilizzare questo per ingannare gli utenti a pensare che stiano visitando un sito web legittimo, quando in realtà stanno visitando un sito web falso.
- ARP Cache Poisoning: la macchina dell'attaccante si finge gateway e quindi tutti il traffico della rete passa per questa.
- Wi-Fi Eavesdropping: un attore malintenzionato intercetta i dati che vengono trasmessi su una rete Wi-Fi non crittografata. Si induce la vittima di connettersi a una rete malevola.
- Email Hijacking: Come suggerisce il nome, in questo tipo di attacco i criminali informatici prendono il controllo delle caselle di posta elettronica per ottenere dati sensibili. Una volta entrati, gli aggressori possono monitorare i dati in transito. Esempio emails di banche e clienti. Nei peggiori casi potrebbero diffondere malware e siti di phishing.

Attacchi comuni

Malware

- virus
- worm
- trojan
- rootkit
- spyware
- adware
- ransomware

Protezione

- antivirus
- controllo dell'hash dei applicativi scaricati
- installare solo da repository ufficiali

Attacchi Web

Alcuni tra i più noti

- sqli
- xss
- csrf
- ssrf
- rce
- dos (dos, drdos)
- enumerations
- brute force

etc...

Gli attacchi e vulnerabilità sono raggruppati ed elencati

- https://owasp.org/
- https://cwe.mitre.org/
- https://www.exploit-db.com/

- https://book.hacktricks.xyz

Attacchi Web

Gli attacchi di tipo ***side channel*** sono un tipo di attacco informatico che sfruttano informazioni collaterali o secondarie per violare un sistema o un'applicazione. In particolare, gli attacchi di tipo side channel si basano sul fatto che l'esecuzione di un'operazione può influenzare il comportamento di un sistema in modo non direttamente correlato all'operazione stessa.

timing attack

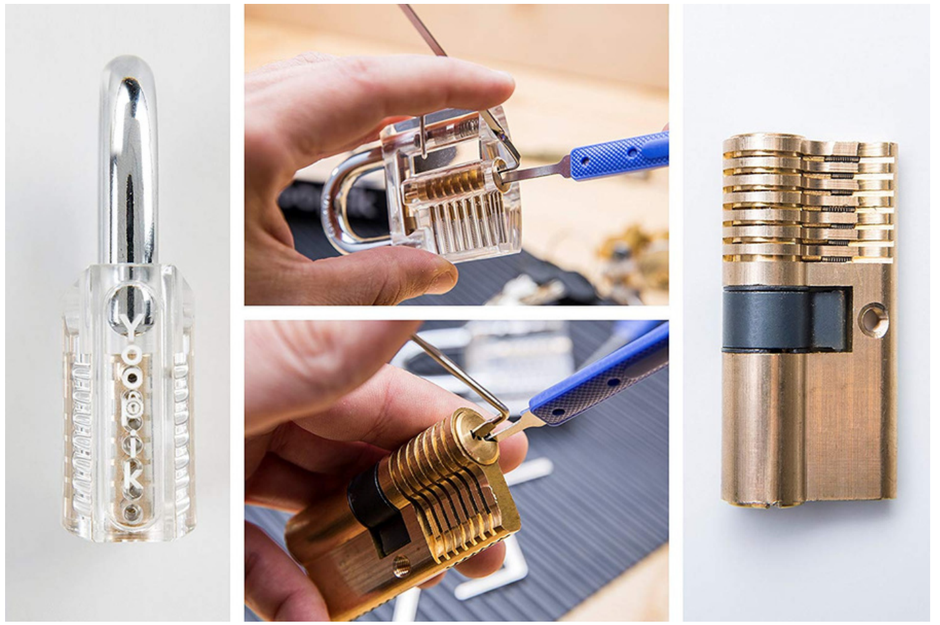
```
if (inputPassword == userPassword) {
return true;
}
```

Attacco **Meltdown e Spectre**: questi attacchi hanno sfruttato vulnerabilità nei processori Intel per recuperare le chiavi di crittografia e altre informazioni sensibili.

Attacchi comuni

Attacchi non tecnologici

- Intrusione
- Scassinamento (lockpicking)
- Danni fisici
- Social Engineering



Attacchi comuni

Social Engineering

Il social engineering è una tecnica di ingegneria sociale che sfrutta le ***vulnerabilità umane*** per ottenere l'accesso a informazioni o sistemi sensibili.

Negli anni '90, il social engineering consisteva nel chiamare al telefono le vittime per indurle a divulgare le proprie credenziali con l'inganno e fornire il numero di rete fissa che consentiva agli hacker di accedere ai server aziendali interni.

Oggi invece il social engineering viene utilizzato per spingere i dipendenti di un’azienda a scaricare file dannosi, visitare siti di phishing, inviare dati e/o file sensibili, ecc.

Kevin Mitnick

- L'arte dell’inganno
- L'arte dell’intrusione
- L’arte dell’hacking

Attacchi comuni

Social Engineering

Una tecnica nota ad esempio quella di spacciarsi per un dipendente o un dirigente di azienda, oppure fingersi un cliente bisognoso di assistenza. L'obbiettivo è ottenere informazioni riservate o modificare le funzionalità di un account.

L'ingegneria sociale fa leva sulla natura umana della vittima, cercando di suscitare timore e senso di urgenza, al fine di impedire che l'utente abbia il tempo per riflettere a sufficienza prima di intraprendere una determinata azione.

- Manipolazione

Phishing: email fraudolente che possono contenere siti di phishing

Vishing e smishing: utilizzo di software per la sintesi vocale, e per la composizione automatica delle chiamate, si effettuano chiamate alle potenziali vittime (da qui il nome vishing, ossia voice phishing), o inviano loro SMS (smishing, ossia sms phishing)

Truffa del CEO: normalmente quando sono i dirigenti a chiedere ai dipendenti di svolgere un determinato compito, è normale per gli utenti avvertire una certa pressione e urgenza nel portare a termine l'incarico. I cybercriminali sfruttano questa attitudine spacciandosi per il direttore o uno dei dirigenti dell'azienda, così da suscitare nella vittima un senso di urgenza che la spinga a compiere l'azione desiderata dai truffatori. Questo tipo di attacco è noto come truffa del CEO.

Tailgating o piggybacking: si verifica nelle grandi aziende, che bloccano l'accesso non autorizzato a determinati locali. Si utilizzano il tailgating o il piggybacking per spingere le vittime ad utilizzare i propri badge così da consentire ai malintenzionati di accedere fisicamente alle aree riservate.

Quid pro quo: in questo caso si fa leva sul malcontento di dipendenti scontenti, che potrebbero essere indotti a fornire informazioni sensibili in cambio di denaro.

Attacchi comuni

Social Engineering

Trashing

L'attacco trashing, o information diving, è una tecnica di ingegneria sociale che consiste nel recuperare informazioni riservate da un bersaglio setacciando i suoi rifiuti. Questo tipo di attacco può essere utilizzato per ottenere informazioni personali, finanziarie o aziendali, che possono essere poi utilizzate per scopi illeciti, come frodi, furti d'identità o spionaggio industriale.

Le informazioni che possono essere recuperate attraverso un attacco trashing sono molteplici e possono includere:

- Dati personali, come nome, indirizzo, numero di telefono, data di nascita, ecc.
- Informazioni finanziarie, come numeri di carte di credito, codici PIN, estratti conto, ecc.
- Informazioni aziendali, come segreti commerciali, piani di marketing, ecc.

Si utilizzano spesso il trashing per ottenere informazioni che possono essere utilizzate per sferrare attacchi informatici più sofisticati. Ad esempio, un hacker potrebbe utilizzare i dati personali di una vittima per creare un falso documento d'identità o per effettuare un furto d'identità.

Per proteggersi dagli attacchi trashing, è importante adottare le seguenti misure di sicurezza:

- Riciclare i rifiuti in modo sicuro, distruggendo tutti i documenti che contengono informazioni riservate.
- Non gettare mai nella spazzatura documenti che contengono informazioni sensibili.
- Tenere i documenti riservati in un luogo sicuro.

Attacchi comuni

Social Engineering

Come difendersi

In ambito aziendale:

- Creare un'infrastruttura di fiducia per gli impiegati e il resto del personale (specificare dove, come, quando e da chi devono essere trattati i dati).
- Capire quali informazioni sono sensibili e valutare il loro livello di esposizione verso l'esterno.
- Stabilire protocolli di sicurezza, politiche e procedure per i dati sensibili.
- Allenare il personale di interesse nelle procedure di sicurezza di interesse.
- Testare casualmente, senza riferirlo, tale infrastruttura.
- Manipolare e revisionare tutti i passaggi.
- Utilizzare un servizio di gestione dei rifiuti con depositi chiusi con lucchetti apribili solamente dal personale di pulizia autorizzato.

A livello personale

- Diffidare da mail o telefonate non sollecitate, specialmente se da parte di persone che chiedono informazioni sui dipendenti o riguardo all'azienda (anche finanziarie). Documentarsi prima su chi richiede tali dati (autorità).
- Non diffondere informazioni sensibili in rete senza verificare il livello di sicurezza e attendibilità del sito.
- Controllare sempre la URL del sito web, poiché potrebbe contenere alcune lievi differenze rispetto all'originale.
- Documentarsi meglio sul mittente del messaggio, senza far riferimento solamente alle informazioni di contatto, ma andando a ricercare i possibili attacchi nelle liste di phishing trovabili tramite motore di ricerca.
- Evitare di aprire allegati o file eseguibili di dubbia provenienza.

Politiche di controllo di accesso: per specificare chi si vuole proteggere, bisogna definire delle regole di accesso e controllare che le regole siano soddisfatte.

Una politica limita le operazioni che gli utenti possono fare, è un set di regole ad alto livello che descrive gli accessi autorizzati al sistema. Questa separazione permette analisi dei requisiti indipendente da implementazione.
Le politiche possono essere descritte in linguaggio naturale (semplice ma impreciso), matematico, o linguaggio ad hoc.

Più politiche possono entrare in conflitto, e generare una vulnerabilità.

Nel controllo accessi, abbiamo il soggetto che richiede accesso, l'oggetto (risorsa), le operazioni/modalità di accesso (da soggetto a oggetto), permessi (possibilità di accedere a risorsa in certa modalità), privilegi (insieme di permessi dati a ruolo come amministratore, operatore..).

Un sistema del controllo accessi regola quindi le operazioni che possono essere eseguite sui dati, prevenendo azioni che potrebbero danneggiare dati o risorse.

Access Control Models

Mandatory Access Control (MAC)
Il controllo di accesso obbligatorio (MAC) è un tipo di controllo di accesso che impone restrizioni all'accesso alle risorse basate su etichette di sicurezza. Le etichette di sicurezza sono assegnate alle risorse e agli utenti e determinano quali utenti possono accedere a quali risorse.

Il MAC è implementato dal sistema operativo e non può essere modificato dagli utenti. Ciò garantisce che le restrizioni di accesso siano applicate coerentemente.
Il MAC è spesso utilizzato in ambienti ad alta sicurezza, come sistemi militari e governativi.

Role-based Access Control (RBAC)
Il controllo di accesso basato sui ruoli (RBAC) è un tipo di controllo di accesso che assegna agli utenti i ruoli e quindi determina i permessi di accesso basati sui ruoli assegnati.

I ruoli sono gruppi di permessi di accesso che vengono assegnati agli utenti in base alle loro responsabilità lavorative. Ad esempio, un utente con il ruolo di "amministratore" potrebbe avere il permesso di accedere a tutte le risorse, mentre un utente con il ruolo di "utente standard" potrebbe avere il permesso di accedere solo alle risorse necessarie per svolgere il proprio lavoro.
L'RBAC è un tipo di controllo di accesso flessibile e facile da gestire. È spesso utilizzato in ambienti aziendali.

Access Control Models

Attribute-based Access Control (ABAC)
Il controllo di accesso basato sugli attributi (ABAC) è un tipo di controllo di accesso che utilizza gli attributi degli utenti e delle risorse per determinare chi può accedere alle risorse.

Gli attributi sono proprietà degli utenti e delle risorse, come il reparto, il ruolo, il tipo di file e la data di creazione. Le regole di accesso vengono valutate in base agli attributi degli utenti e delle risorse per determinare se un utente ha accesso a una risorsa.
L'ABAC è un tipo di controllo di accesso potente e flessibile. È spesso utilizzato in ambienti cloud e multi-cloud.

Discretionary Access Control (DAC)
Il controllo di accesso discrezionale (DAC) è un tipo di controllo di accesso che consente ai proprietari delle risorse di determinare chi può accedere alle proprie risorse.

I proprietari delle risorse possono concedere o negare l'accesso alle proprie risorse ad altri utenti. Ad esempio, un proprietario di un file può concedere il permesso di lettura ad altri utenti, ma negare il permesso di scrittura.
Il DAC è un tipo di controllo di accesso semplice e flessibile. È spesso utilizzato in ambienti non protetti, come sistemi domestici e di piccole imprese.

Rule-based Access Control (RuBAC)
Il controllo di accesso basato sulle regole (RuBAC) è un tipo di controllo di accesso che utilizza regole per determinare chi può accedere alle risorse. Le regole sono espressioni logiche che vengono valutate per determinare se un utente ha accesso a una risorsa. Ad esempio, una regola potrebbe consentire l'accesso a una risorsa solo agli utenti che sono membri di un determinato gruppo e che hanno un determinato ruolo.
Il RuBAC è un tipo di controllo di accesso potente e flessibile. È spesso utilizzato in ambienti ad alta sicurezza, come sistemi militari e governativi.

Risorse utili

- https://auth0.com/
- https://casbin.org/
- https://casdoor.org/

- https://owasp.org/
- https://cwe.mitre.org/
- https://www.exploit-db.com/

- https://book.hacktricks.xyz