# Cyber Security e Crittografia,le origini e l'evoluzione

Internet,o ad essere più precisi il suo antenato,non è nato per necessità dovute alla guerra,ma bensì grazie a quella rivalità che si era venuta a creare con la Russia nella famosa 'lotta allo spazio' degli anni sessanta. L'idea fu dell'allora presidente degli stati uniti,Eisenhower.
Egli era spaventato dal lancio dal vantaggio che la russia stava acquisendo e temendo di perdere l'egemonia in campo economico,scientifico e tecnologico ha capito di dover rispondere in maniera decisa,chiamò quindi a sé il direttore del MIT e lo mise a capo del progetto ARPA.
L'idea era di creare una rete di computer in comunicazione tra loro per evitare gli spostamenti,ma bisognava trovare il modo di far parlare i computer tra di loro.
Nel 1969,dopo numerose ricerche,venne realizzato il primo collegamento tra un computer dell'Università della California e uno a Palo Alto. Era il 29 Ottobre ed era finalmente nata Arpa Net.
Di Web invece si comincia a parlare solo negli anni novanta,una "rivoluzione digitale" portata avanti grazie al CERN di ginevra,i cui ricercatori diedero vita poi successivamente al World Wide Web.
Questa rivoluzione venne accompagnata da persone che durante il corso del tempo hanno interpretato diversi ruoli: gli Hacker.
Infatti inizialmente vennero riconosciuti come esperti informatici e programmatori,solo successivamente il termine hacker assunse diverse sfaccettature,a causa della sempre più grande diffusione di internet e computer. Proprio per questo motivo andò perduto il codice etico degli hacker, e i programmatori più giovani iniziarono a sperimentare le proprie capacità con finalità anche dannose creando e diffondendo virus, facendo irruzione nei sistemi informatici militari, provocando deliberatamente il blocco di macchine.
Per questo in seguito a questi primi incidenti,nonostante la la figura dell'hacker era ormai radicata e riconosciuta come esperto programmatore al servizio di aziende e governi,per la maggioranza dei giornalisti e della gente comune egli divenne sinonimo di criminale.
Ovviamente questa credenza è errata,ormai per definire un hacker è necessario fare una differenza tra i termini:

- **white hat hacker**: Si tratta di hacker etici che usano le loro capacità di programmazione per scopi buoni, etici e legali. Possono eseguire test di penetrazione della rete nel tentativo di compromettere le reti utilizzando la loro conoscenza dei sistemi di sicurezza informatica per scoprire le vulnerabilità della rete. Le vulnerabilità di sicurezza vengono poi segnalate agli sviluppatori affinché le risolvano prima che le vulnerabilità possano essere sfruttate
- **gray hat hacker**: Si tratta di individui che commettono reati e fanno cose probabilmente senza seguire un'etica, ma non per guadagno personale o per causare danni. Un esempio potrebbe essere quello di qualcuno che compromette una rete senza autorizzazione e poi rivela pubblicamente la vulnerabilità.
- **black hat hacker**: Si tratta di criminali che non seguono nessuna etica che violano la sicurezza dei computer e delle reti per guadagno personale, come ad esempio l'attacco alle reti. I black hat hacker sfruttano le vulnerabilità per compromettere i sistemi informatici e di rete.

Buono o cattivo, l'hacking è un aspetto importante della sicurezza della rete.
Al fine di proteggersi da questa nuova categoria di programmatori, fu necessario introdurre sistemi di sicurezza e insiemi di regole che andarono a comporre quella grande macchina in continua evoluzione che è oggi la **CyberSecurity**.
Più precisamente questo termine si riferisce a un insieme di comportamenti,mezzi e tecnologie volti alla protezione di sistemi informatici,garantendo disponibilità,confidenzialità e integrità.
Con **integrità** si intende la capacità di impedire che i nostri dati vengano modificati da qualcuno senza autorizzazione.
Con **disponibilità** la possibilità di accedere ai nostri dati quando ne abbiamo bisogno,questa può venire a mancare a causa di attacchi DoS,per blackout o malfunzionamenti.
Mentre con **confidenzialità** si intende la capacità di proteggere i nostri dati e non mostrarli a persone non autorizzate.
Dai tempi dei primi hacker siamo arrivati al giorno d'oggi dove ci sono vari tipi di aggressori, tra cui i **dilettanti** che attaccano per divertimento e prestigio, gli **hacktivisti** che operano per promuovere una causa politica e gli **hacker professionisti** che attaccano per profitto. Inoltre, le nazioni possono attaccare altre nazioni per ottenere un vantaggio economico attraverso il furto di informazioni, o per danneggiare o distruggere i beni di un altro paese(Da qui il concetto della CyberWarfare).
Nella difesa di una rete bisogna conoscere questi termini fondamentali:

- **Minaccia** - Un potenziale pericolo per i dati o la rete stessa.
- **Vulnerabilità** - Un punto debole di un sistema che potrebbe essere sfruttato da una minaccia. lo "spazio d'attacco" consiste nell vulnerabilità di un determinato sistema e descrive diversi punti in cui una persona può entrare.
- **Exploit** - Il meccanismo che viene utilizzato per sfruttare una vulnerabilità per compromettere una risorsa. Gli exploit possono essere remoti o locali. Un exploit remoto è un exploit che funziona sulla rete senza alcun accesso preliminare al bersaglio.. In un exploit locale,l'attaccante ha un qualche tipo di accesso al sistema.
- **Rischio** - La probabilità che una particolare minaccia sfrutti una particolare vulnerabilità di un sistema e produca conseguenze indesiderate.

La prima contromisura che viene presa contro un attacco informatico è la cosiddetta analisi del rischio,essa parte dall'identificazione dei beni da proteggere per poi valutare le possibili minacce in termini di gravità del danno. In base alla stima del rischio si decide se, come e quali contromisure di sicurezza adottare.
Ci sono quattro modi comuni per gestire il rischio:

- **Accettazione del rischio** - È quando il costo delle opzioni di gestione del rischio supera il costo del rischio stesso. Il rischio viene accettato senza azione

- **Evitare il rischio** - Si tratta di un'azione che evita qualsiasi esposizione al rischio. Questa è di solito l'opzione di mitigazione del rischio più costosa.

- **Limitazione del rischio** - Limita l'esposizione al rischio di un'azienda intraprendendo qualche azione. È la strategia di mitigazione del rischio più comunemente usata

- **Trasferimento del rischio** - Il rischio viene trasferito a una terza parte volontaria

Spesso l'obiettivo dell'attaccante non è rappresentato dai sistema informatici in sè ma piuttosto dai dati in essi contenuti.

La sicurezza informatica deve quindi preoccuparsi di impedire l'accesso sia agli utenti non autorizzati che ai soggetti con privilegi limitati, per evitare che i dati appartamenti al sistema informatico vengano copiati,modificati o cancellati. Le violazioni possono essere molteplici,vi possono essere tentativi non autorizzati di accesso a zone riservate,furto di identità digitale o di file riservati.
I danni spesso sono causati accidentalmente dall'utente stesso a causa di una cattiva implementazione di hardware e software,da interruzioni di servizio o guasti imprevisti. Per evitare gli eventi accidentali non esistono soluzioni definitive: un primo rimedio è il backup del sistema, dei dati e delle app.
I nostri dispositivi sono particolarmente soggetti ad attacchi di malware. Si tratta di codice o software specificamente progettato per danneggiare, interrompere, rubare o, in generale, infliggere qualche altra azione "cattiva" o illegittima su dati, host o reti. È importante conoscere il malware perché gli attori della minaccia e i criminali online cercano spesso di ingannare gli utenti per installare malware che aiutano a sfruttare buchi nella sicurezza. Inoltre, il malware si trasforma così rapidamente che gli incidenti di sicurezza legati ad essi sono estremamente comuni perché i software anti malware non possono essere aggiornati abbastanza rapidamente da fermare le nuove minacce.
Il primo dei Malware è il **virus**,esso è un tipo di malware che si propaga inserendo una copia di se stesso in un altro programma. I virus si diffondono poi da un computer all'altro, infettando i computer.
Poi ci sono i **Trojan**,un software che sembra essere legittimo, ma contiene codice maligno che sfrutta i privilegi dell'utente che lo esegue.
Il trojan può causare danni immediati, fornire l'accesso remoto al sistema o l'accesso attraverso una backdoor. Può anche eseguire azioni da remoto, come farsi inviare password e dati ad intervalli di tempo regolari.
Successivamente ci sono i **worm** ,essi sono simili ai virus perché si replicano e possono causare lo stesso tipo di danno. In particolare, i worm si replicano sfruttando in modo indipendente le vulnerabilità delle reti. I worm possono rallentare le reti mentre si diffondono da un sistema all'altro.
Infine c'è il **ransomware**. Esso è un malware che nega l'accesso al sistema informatico infetto o ai suoi dati. I criminali informatici chiedono poi un pagamento per liberare il sistema informatico dal ransomware.

Altri malware altrettanto conosciuti sono:

- **Spyware** - utilizzato per raccogliere informazioni sull'utente
- **Adware** - mostra dei pop-up per generare entrate per il suo autore. Il malware può analizzare gli interessi dell'utente tracciando i siti web visitati. Può quindi inviare pop-up pubblicitari pertinenti a quei siti.
- **Scareware** - utilizza il social engineering per creare messaggi di paura che spingono l'utente a installare software dannosi
- **Phishing** - tenta di convincere le persone a divulgare informazioni sensibili.
- **Rootkit** - Questo malware è installato su un sistema compromesso. Dopo l'installazione, continua a nascondere la sua intrusione e a fornire un accesso privilegiato all'Hacker.

La lista continuerà a crescere con l'evoluzione di Internet. Verranno sviluppati sempre nuovi attacchi. Uno dei principali obiettivi delle operazioni di cyber Security è quello di conoscere i nuovi malware e porvi rimedio.

Altri tipi di attacco possono essere L'attacco **DoS**,che punta su una rete di zombie per impedire la regolare fruizione di un servizio,l'utilizzo di **keylogger**,per il furto di password,il **social engineering** che avviene sui social e sfrutta la possibilità di fingersi qualcun altro per effettuare truffe online.
Quando sono stati redatti gli standard di Internet, nessuno pensava che i dati dovessero essere protetti,ma come si è visto nel corso degli anni i nostri sistemi sono vulnerabili a diversi attacchi.
Per affrontare queste vulnerabilità, utilizziamo una varietà di tecnologie crittografiche per mantenere i nostri dati privati e sicuri. Tuttavia, la crittografia è una spada a doppio taglio in quanto gli Hacker possono anche usarla per nascondere le loro azioni.
La crittologia combina due discipline separate:

- **Crittografia** - è la pratica e lo studio delle tecniche per rendere sicure le comunicazioni.
- **Crittoanalisi** - È la rottura di quei codici creati con la crittografia. In particolare lo studio dei punti deboli delle tecniche crittografiche.

C'è una relazione tra le due discipline perché ognuna rende l'altra più forte. Le organizzazioni di sicurezza nazionale impiegano professionisti di entrambe le discipline e le mettono l'una contro l'altra.
la crittografia però non è qualcosa che è nata con la tecnologia,infatti già secoli fa sono stati utilizzati vari metodi di crittografia, dispositivi fisici e ausili per crittografare e decrittografare il testo. Gli esempi storici di cifratura sono:Scitala,cifrario di cesare,cifrario di Vigenère e la macchina Enigma.
Ognuno di questi metodi di cifratura utilizza un algoritmo specifico, chiamato cifrario.
Un cifrario è un algoritmo che consente di codificare e decodificare un messaggio.

La crittoanalisi invece è spesso utilizzata dai cybercriminali per decifrare messaggi criptati, ma è utilizzata anche dai governi nella sorveglianza militare e dalle imprese per testare la forza delle procedure di sicurezza.
I crittoanalisti sono persone che eseguono crittoanalisi per decifrare codici segreti.In crittoanalisi vengono utilizzati diversi metodi:

- **metodo brute force** - Il crittoanalista prova ogni possibile chiave sapendo che alla fine uno di essi funzionerà. Alla fine se ogni possibile chiave viene provata, una delle chiavi deve funzionare,nonostante questo richieda un'enorme capacità di calcolo.

- **metodo Ciphertext** - Il crittoanalista ha il cifrario di diversi messaggi criptati ma non conosce il testo in chiaro sottostante.

- **Metodo Meet-in-the-Middle** - Il crittoanalista conosce una parte del testo in chiaro e il corrispondente testo cifrato.

**L'autenticazione, l'integrità e la confidenzialità** sono implementate in molti modi, utilizzando vari protocolli e algoritmi.

Per verificare e garantire l'integrità e l'autenticazione dei dati vengono utilizzati gli **hash** vengono utilizzati per verificare e garantire l'integrità dei dati.
Una funzione di hash prende un blocco di dati binari, chiamato messaggio, e produce una rappresentazione condensata a lunghezza fissa, chiamata hash. L'hash risultante è anche chiamato talvolta digest, o impronta digitale.
Con le funzioni di hash, è impossibile che due diversi gruppi di dati producano lo stesso risultato di hash. Ogni volta che i dati vengono modificati o alterati, cambia anche il valore dell'hash.
Ci sono tre note funzioni di hash: MD5,SHA-1,SHA-2

Per garantire la riservatezza dei dati usiamo invece:

- **Algoritmi di cifratura simmetrica** - utilizzano la stessa chiave per cifrare e decifrare i dati. Si basano sulla premessa che ogni parte comunicante conosca la chiave pre-condivisa. Gli algoritmi di uso comune utilizzano uno sei seguenti sistemi:DES,3DES,AES,SEAL
- **Algoritmi di cifratura asimmetrici** - utilizzano chiavi diverse per cifrare e decifrare i dati,a chiave pubblica che deve essere distribuita e la chiave privata,personale e segreta.
  Esempi di protocolli che utilizzano algoritmi a chiave asimmetrica includono: IKE,SSH,SSL

Infine l'ultimo concetto che è importante accennare nella crittografia sono le firme digitali,esse sono comunemente usate nelle situazioni seguenti:

- **Firma del codice** - utilizzata per verificare l'integrità dei file scaricati dal sito web di un fornitore
- **Certificati digitali** - Sono simili a una carta d'identità virtuale e vengono utilizzati per autenticare l'identità del sistema.

Per concludere,potremmo dilungarci in tecnicismi e discorsi complessi ma credo che la conclusione alla quale arriviamo è che tutti dovremmo sviluppare una buona consapevolezza della sicurezza informatica. La sicurezza informatica è una responsabilità condivisa che tutti gli utenti devono mettere in pratica. Ad esempio, dobbiamo segnalare i crimini informatici alle autorità competenti, essere consapevoli delle potenziali minacce presenti nel web e proteggere le informazioni importanti dai furti. Le organizzazioni devono agire e proteggere le proprie risorse, gli utenti e i clienti.
Se a proteggere i nostri dati non contribuiamo noi in prima linea,come possiamo sperare di rendere internet e il web una realtà migliore e accessibile a tutti?