Axhenti alessandro

SISTEMI E RETI

Crittografia

La Crittografia: Fondamenti, Attacchi e Algoritmi

Introduzione

La crittografia è una disciplina della sicurezza informatica che si occupa di trasformare le informazioni per renderle incomprensibili a chi non è autorizzato. Il suo obiettivo principale è garantire **confidenzialità, integrità, autenticazione e non ripudio**.

Le moderne tecniche crittografiche vengono utilizzate in numerosi ambiti, tra cui:

- **Protezione delle password** nei database.
- **Crittografia delle comunicazioni** in reti sicure come VPN e HTTPS.
- **Sicurezza nelle transazioni bancarie online**.
- **Protezione delle firme digitali** per garantire l'autenticità dei documenti.

Sebbene la crittografia sia molto efficace, esistono attacchi in grado di compromettere la sicurezza di un sistema. Per questo motivo, è fondamentale comprendere non solo i principi base della crittografia, ma anche le minacce e le tecniche di protezione.

---

1. Attacchi alla Crittografia

La crittografia protegge i dati, ma non è immune agli attacchi. Esistono diverse strategie per tentare di violarla, alcune basate sulla forza bruta, altre sull'analisi matematica dei sistemi crittografici. Vediamo nel dettaglio alcuni degli attacchi più diffusi.

1.1 Attacco a Forza Bruta

Un attacco a forza bruta consiste nel provare tutte le combinazioni possibili di una chiave fino a trovare quella corretta. La sua efficacia dipende dalla lunghezza della chiave:

- **Chiavi a 56 bit (DES)** → vulnerabili in poche ore.
- **Chiavi a 128 bit (AES)** → richiederebbero miliardi di anni con la tecnologia attuale.

Un modo per contrastare questo attacco è aumentare la lunghezza delle chiavi o utilizzare algoritmi che rallentano il processo di autenticazione (es. Argon2 per le password).

1.2 Attacco a Dizionario

Simile alla forza bruta, ma invece di provare tutte le combinazioni, l'attaccante utilizza un elenco di parole comuni o frasi probabili (es. "password123", "admin", "qwerty"). Questo attacco è molto efficace contro password deboli.

Protezione:

- Utilizzare password complesse e lunghe.
- Impiegare tecniche di hashing sicuro (come bcrypt o Argon2) per rendere le password difficili da recuperare.

1.3 Attacco Man-in-the-Middle (MITM)

L'attaccante si interpone tra due interlocutori e intercetta o modifica i dati in transito. Questo può avvenire in diversi modi:

1° **Intercettazione di una comunicazione HTTP non cifrata:** l'attaccante legge le informazioni trasmesse.

2° **Attacco SSL Strip:** un hacker forza una connessione HTTPS a diventare HTTP, rendendo visibili le informazioni trasmesse.

3° **DNS Spoofing:** l'attaccante modifica le risposte DNS per dirottare la vittima su un sito fasullo.

Protezione:

- Usare HTTPS e VPN per cifrare le comunicazioni.
- Verificare i certificati digitali.
- Utilizzare autenticazione a due fattori (2FA).

1.4 ARP Spoofing

L'ARP Spoofing è un attacco a livello di rete locale (LAN) in cui un hacker invia falsi messaggi ARP per associare il proprio indirizzo MAC all'indirizzo IP di un altro dispositivo. In questo modo, tutto il traffico destinato alla vittima passerà attraverso l'attaccante, permettendogli di intercettare password, sessioni di login e dati sensibili.

Protezione:

- Utilizzo di ARP statici per evitare aggiornamenti non autorizzati.
- Abilitazione di **Port Security** sugli switch.
- Monitoraggio della rete con strumenti come **Wireshark**.

---

2. Tipi di Crittografia

Esistono due principali categorie di crittografia: **simmetrica** e **asimmetrica**.

2.1 Crittografia Simmetrica

Utilizza **una sola chiave** per cifrare e decifrare i dati. È molto veloce ed efficiente, ma presenta il problema della condivisione sicura della chiave.

Esempi di algoritmi:

AES (Advanced Encryption Standard)

- Chiavi di **128, 192 o 256 bit**.
- Basato su operazioni matematiche avanzate chiamate **S-Box** e **MixColumns**.
- Sicuro e usato in reti Wi-Fi, VPN e documenti protetti.

DES (Data Encryption Standard) - Obsoleto

- Chiave di **56 bit**, ormai vulnerabile a forza bruta.
- Sostituito da AES e 3DES.

RC4 - Obsoleto

- Algoritmo a flusso usato in passato per proteggere HTTPS e Wi-Fi.
- Ora considerato insicuro per vulnerabilità nell'output del keystream.

2.2 Crittografia Asimmetrica

Utilizza **una coppia di chiavi**:

- **Chiave pubblica:** usata per cifrare.
- **Chiave privata:** usata per decifrare.

Esempi di algoritmi:

RSA (Rivest-Shamir-Adleman)

- Basato sulla fattorizzazione di numeri primi.
- Sicuro con chiavi di almeno **2048 bit**.
- Utilizzato in SSL/TLS, email cifrate e firme digitali.

ECC (Elliptic Curve Cryptography)

- Alternativa più efficiente a RSA.
- Offre la stessa sicurezza con chiavi più corte (256 bit ECC = 3072 bit RSA).
- Utilizzato in sistemi embedded e dispositivi mobili.

---

3. Algoritmi di Hashing

Gli algoritmi di hashing trasformano un dato in una stringa univoca e irreversibile. Sono usati per proteggere password e verificare l'integrità dei dati.

Esempi di algoritmi:

MD5 - Obsoleto

- Genera un hash a **128 bit**.
- Vulnerabile agli attacchi di collisione.

SHA-1 - Obsoleto

- Genera un hash a **160 bit**.
- Compromesso da attacchi nel 2017.

SHA-256 (Sicuro)

- Genera un hash a **256 bit**.
- Utilizzato in blockchain e crittografia avanzata.

Argon2 (Consigliato per password)

- Progettato per resistere agli attacchi di forza bruta.
- Utilizzato nei moderni gestori di password.

---

4. Protocolli di Scambio Chiavi

Uno dei problemi principali della crittografia è **lo scambio sicuro delle chiavi**.

Diffie-Hellman (DH)

- Permette a due parti di generare una chiave segreta su un canale insicuro.
- Vulnerabile agli attacchi **Man-in-the-Middle** senza autenticazione.

ECDH (Elliptic Curve Diffie-Hellman)

- Variante più sicura di DH basata sulle curve ellittiche.
- Meno vulnerabile agli attacchi quantistici.