Azzolini Riccardo 2021-03-01

Tecniche di crittografia

1 Caratteristiche dei sistemi crittografici

Oltre che dal numero di chiavi utilizzate, i sistemi crittografici sono caratterizzati da:

- Le operazioni usate per la cifratura;
  - La cifratura simmetrica si basa su sostituzioni e/o trasposizioni dei (gruppi di) bit che costituiscono il testo in chiaro. Queste operazioni possono essere implementate in modo molto efficiente, a livello software o hardware.
  - La cifratura asimmetrica si basa su particolari funzioni matematiche, che tendono a essere piuttosto costose da calcolare.
- Il metodo con cui viene elaborato il testo in chiaro:
  - **A blocchi**: il testo in chiaro viene suddiviso in blocchi di dimensione fissa (ad esempio 64, 128 o 256 bit), poi ogni blocco di testo in chiaro viene trasformato in un blocco di testo cifrato. Questa è la tecnica di cifratura più utilizzata: funzionano in questo modo i sistemi di cifratura simmetrici DES e AES, il sistema di cifratura asimmetrico RSA, e tanti altri.
  - **A flusso** (**stream**): il messaggio viene cifrato/decifrato bit a bit (o byte a byte, o in generale lavorando sull'unità di misura più piccola considerata), senza bisogno di bufferizzarlo fino ad accumulare un intero blocco di dimensione fissa. Come si vedrà più avanti, ci sono dei modi di usare un algoritmo a blocchi per operare su un flusso.

2 Tipi di attacchi nei sistemi crittografici

Lo scopo principale di un attacco è quello di *ricostruire la chiave* utilizzata, piuttosto che semplicemente decifrare un messaggio: una volta ricostruita la chiave, l'attaccante acquisisce il controllo del canale di comunicazione, ovvero può leggere tutti i messaggi che vi transitano (purché la chiave utilizzata non venga sostituita con una nuova).

Esistono due principali tipi di attacchi: *crittoanalisi* e *forza bruta*.

2.1 Crittoanalisi

La **crittoanalisi** sfrutta le caratteristiche dell'algoritmo di cifratura e la conoscenza di testi in chiaro e/o testi cifrati per tentare di individuare la chiave. Per poter effettuare attacchi di questo tipo, l'attaccante deve conoscere l'algoritmo di cifratura utilizzato, ma ciò in pratica è sempre vero, perché gli algoritmi crittografici *devono* essere pubblici, al fine di:

- permettere alla comunità (in particolare, ai ricercatori) di analizzarlo per determinare se è robusto, resistente agli attacchi noti;
- consentirne l'implementazione, a livello sia software che hardware, da parte di più vendor.

Gli attacchi di crittoanalisi sono classificati in base a ciò che l'attaccante conosce:

- **solo testo cifrato** (**ciphertext only**): si conoscono solo l'algoritmo e il testo cifrato;
- **testo in chiaro conosciuto** (**known plaintext**): si conoscono l'algoritmo e delle coppie di testi in chiaro e testi cifrati corrispondenti;
- **testo in chiaro selezionato** (**chosen plaintext**): si conoscono l'algoritmo e delle coppie di testi in chiaro e testi cifrati corrispondenti, dove i testi in chiaro sono stati scelti dall'attaccante.

Un attacco con testo in chiaro conosciuto può spesso essere effettuato determinando il protocollo usato per la comunicazione segreta e sfruttando i contenuti standard (header, ecc.) dei messaggi di tale protocollo.

Invece, un attacco con testo in chiaro selezionato è tipicamente molto più difficile, perché l'attaccante deve in qualche modo "convincere" una delle entità comunicanti a cifrare dei dati forniti dall'attaccante stesso. Il vantaggio di questo attacco è che il testo in chiaro può essere scelto in modo da fornire le massime informazioni possibili sulla chiave di cifratura.

Gli algoritmi di cifratura devono essere progettati in modo da essere resistenti agli attacchi di crittoanalisi. Ad esempio, l'algoritmo DES (Data Encryption Standard) è teoricamente vulnerabile a un attacco chosen plaintext, ma in pratica tale attacco non è fattibile, perché richiede che vengano cifrati con la stessa chiave ben 2^{47} messaggi scelti dall'attaccante, e qualunque sistema ben progettato dovrebbe cambiare la chiave dopo averla impiegata per un numero molto inferiore di messaggi.

2.2 Forza bruta

Un **attacco a forza bruta** (**brute force**) consiste nel tentare ogni possibile chiave (si dice "esplorare tutto lo spazio delle chiavi") su un frammento di testo cifrato, finché non si riesce a ottenere una decifratura corretta.

Questo attacco è praticamente sempre possibile, perché l'unica condizione necessaria è che l'attaccante sia in grado di riconoscere il testo in chiaro "corretto": quando si prova una chiave errata, l'algoritmo di decifratura non dà un errore, ma piuttosto produce un output che non è il vero testo in chiaro, e l'attaccante deve potersene accorgere. Come caso limite, se il testo in chiaro fosse una sequenza di bit completamente casuale (non conosciuta dall'attaccante), allora qualunque output dell'algoritmo di decifratura potrebbe essere quello corretto.

Il principale limite degli attacchi a forza bruta è il tempo necessario, che è proporzionale alla dimensione della chiave: supponendo che tutte le chiavi siano equiprobabili, in media è necessario provare il 50~% delle chiavi prima di riuscire a decifrare il messaggio, quindi per chiavi di n bit servono mediamente 2^{n-1} tentativi. Il tempo che ciascun tentativo richiede dipende poi dalla potenza di calcolo disponibile. Ad esempio, l'algoritmo DES usa chiavi di 56 bit, ovvero ha $2^{56} \approx 7.2 \cdot 10^{16}$ possibili chiavi, dunque un attacco brute force richiederebbe in media $2^{55} \approx 3.6 \cdot 10^{16}$ tentativi:

- eseguendo un tentativo ogni microsecondo, l'attacco impiegherebbe circa 1142 anni;
- eseguendo un milione di tentativi ogni microsecondo (un numero realistico per un'architettura di calcolo distribuita), l'attacco impiegherebbe solo 10 ore.

Invece, con chiavi di 128 bit (usate, ad esempio, dall'algoritmo AES, Advanced Encryption Standard), anche eseguendo un milione di tentativi ogni microsecondo una attacco a forza bruta richiederebbe circa $5.4 \cdot 10^{18}$ anni. Tuttavia, è ragionevole supporre che la potenza di calcolo continui ad aumentare nel tempo, perciò un attacco a forza bruta che non è attualmente praticabile potrebbe diventare fattibile in futuro.

3 Sicurezza di uno schema crittografico

Uno schema crittografico è definito:

- **incondizionatamente sicuro** se non è possibile risalire alla chiave indipendentemente dalla potenza computazionale a disposizione, in quanto il testo cifrato non contiene informazioni sufficienti per permettere all'attaccante di determinare il testo in chiaro, quindi risultano impossibili sia gli attacchi di crittoanalisi che gli attacchi a forza bruta;

- **computazionalmente sicuro** se con le risorse computazionali attualmente a disposizione, non è possibile risalire alla chiave in un tempo utile per l'attacco, cioè se ogni possibile attacco richiede un tempo maggiore del tempo di validità del segreto protetto dalla cifratura (ad esempio, il fatto che un messaggio cifrato con DES possa essere decifrato in qualche ora non è un problema se il contenuto del messaggio è un codice di accesso valido solo per pochi minuti).

Esiste un solo schema crittografico che si è dimostrato essere incondizionatamente sicuro, ma esso ha delle caratteristiche che lo rendono difficile da utilizzare (in particolare, esso è un algoritmo simmetrico che richiede una chiave lunga quanto il messaggio, generata in modo totalmente casuale e utilizzabile una volta sola: se si ha un modo sicuro di inviare la chiave, questo potrebbe invece essere usato per inviare direttamente il messaggio). Di conseguenza, nella maggior parte della applicazioni pratiche si usano schemi crittografici computazionalmente sicuri.