Computer and Network Security

Lorenzo Rossi

December 26, 2021

Contents

Part I

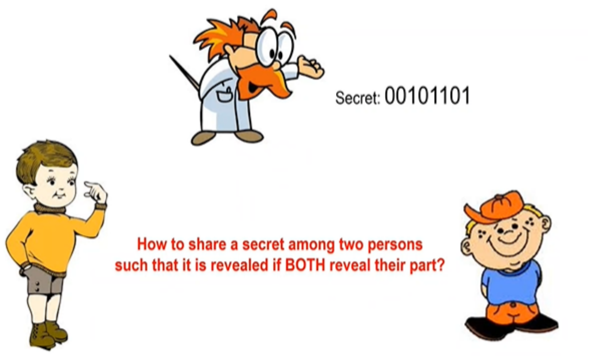
Third Midterm

Chapter 1

Secret Sharing

1.1 Trivial Secret Sharing

Supponiamo di avere un segreto e vogliamo dividerne la conoscenza in due persone (dette shareholders). Inoltre, vogliamo si viene a conoscenza del segreto se e solo se entrambe le parti rivelano la loro porzione di segreto. Chi



fornisce il segreto viene detto **dealer**, mentre chi riceve le porzioni del segreto sono detti **share**.
Nel caso in cui avessimo diviso il segreto in parti uguali, è una pessima idea poiché per indovinare il segreto abbiamo $\frac{1}{2^{N_{bit}}}$ probabilità di indovinare la password ed ora, avendo diviso il segreto in parti uguali, abbiamo una probabilità molto maggiore $\frac{1}{2^{\frac{N_{bit}}{2}}}$.

1.1.1 XOR Secret Sharing

Possiamo fare di meglio:

1. Prendi il segreto i.e.0010.1101;
2. Genera una sequenza casuale **key** i.e.1011.0100;
3. XOR il segreto e il valore casuale **one time pad** i.e.1001.1001;
   Fino ad ora abbiamo applicato un *Vernam cipher*.
4. Diamo ad uno share la sequenza casuale, mentre ad un altro diamo il valore dello XOR;
5. L'unione fra gli share da la chiave.

Importante. *Il conoscere la chiave, cioè il valore casuale, non mi da alcuna informazione riguardante la chiave.*
Lo stesso discorso vale per il valore dello XOR poiché, come dimostrato nel ***perfect secrecy****, l'operatore di XOR tra una stringa pseudocasuale e un valore casuale non da informazioni su quale sia la password.*
Questi due aspetti rappresentano un requisito di sicurezza.

1.1.2 Modular Secret Sharing

Un altro possibile schema è quello di utilizzare le somme modulari:

1. Prendi il segreto S in bit, trasformalo in digit i.e.0010.1101$rightarrow$45;
2. Genera $RAND \mod N$ i.e.$RAND \mod 256 \to 180$;
3. Esegui $S - RAND \mod N$ i.e. $S - RAND \mod 256 \to 121$;

Importante. *Questo schema è equivalente ad One Time Pad poiché abbiamo sommato un numero pseudocasuale con un numero casuare (in modulo). In altre parole, la probabilità di indovinare S conoscendo il valore casuale o il valore della somma è uguale alla probabilità di indovinare senza sapere nulla.*

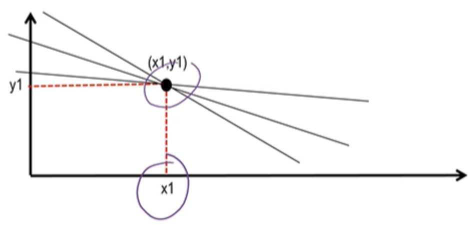
Questo metodo è più facile da implementare per essere condiviso con N shareholders. In particolare, genero 3 quantità truly random ed effettua la differenza tra il segreto e queste 3 quantità modulo N. Nel caso un attacker, riuscisse ad ottenere un numero sufficiente di share non può comunque ottenere la password, ma al più la differenza tra il segreto e le shares non prese.
Da qui è possibile definire il concetto di **perfect secrecy**: un avversario, conoscendo n-1 shares deve ancora possedere la probabilità di indovinare il segreto pari a quella di indovinare il segreto da zero.

1.1.3 Shamir Secret Sharing

Fino ad ora abbiamo costruito uno schema detto (n,n) secret sharing scheme in cui il primo parametro è il numero delle persone necessarie a rilevare il segreto e il secondo parametor è il numero di parti:il segreto viene rilevato solo se tutte le n parti forniscono il segreto.
Un altro schema è (t,n) secret sharing scheme:il segreto è rilevato quando qualsiasi t delle n parti fornisce il segreto. Questo secondo problema è molto più complicato del trivial secret sharing.

Idea:Schema (2,n)

Il problema è quello di modellare uno schema per cui, conoscendo 2 degli n shareholders, posso ricostruire il segreto. Questo problema è riconducibile a quello di conoscere quanti punti sono necessari per definire una linea:ovviamente 2. Infatti conoscendo un solo punto (shares) ho infinite rette passanti per quel punto e quindi è impossibile ricondurci



al segreto;tuttavia, conoscendo 2 punti (shares), tra essi passa solamente una sola retta e conseguentemente posso conoscere il segreto. Abbiamo comunque mantenuto la proprietà di poter avere un numero maggiore di 2 per ottenere il segreto, ma al minimo sono 2.

Procedura: Generalizzazione schema$(2, n)$

- **Dealer:** costruisce la linea:
  1. Coefficiente a:scelto casualemnte;
  2. Segreto S:noto;

  $$y = S + ax$$

  Per esempio: $a = 15 \quad S = 39$
- Distribuisci le shares ai n partecipanti scegliendo casualmente il valore x_i da introdurre nell'equazione della retta:
  - Shareholder 1: $x_1 = 1 \to share = (1, 54)$;
  - Shareholder 2: $x_2 = 2 \to share = (2, 69)$;
  - Shareholder 3: $x_3 = 3 \to share = (3, 84)$;
  - ...

Importante. *La y viene calcolata in base alla funzione della retta;tuttavia, i punti degli shareholder sono mantenuti con (x,y) e il valore delle x_i possono essere noti a priori a patto che la y sia nascosta.*

Procedura: Ricostruzione

- Ricezione di due shares:$P_i = (x_i, y_i) \quad P_j = (x_j, y_j)$;

SONO ARRIVATO A CNS 24: 0:44:11