Protocolli a conoscenza zero

Carlo De Vittoria

PROBLEMI

Dati A, l'utente che si vuole autenticare, e B il sistema di autenticazione

Con le precedenti autenticazioni abbiamo riscontrato i seguenti problemi:

- ✘ **Autenticazione debole**: Conoscendo la password B può impersonare A
- ✘ **Autenticazione forte**: Attraverso un protocollo di sfida e risposta si possono ottenere informazioni riguardanti l'autenticazione (choosen text attack)

Sia A che B sono in possesso di K!

- ✓ **Zero Knowledge**: nessuno scambio di informazioni che possano essere riutilizzate! Solo A conosce k

IDEA

L’ idea è questa:

- l’obbiettivo di chi si vuole autenticare è quello di convincere il sistema di autenticazione di un asserzione (detta “prova (o dimostrazione) di conoscenza”).
- Il sistema può accettare o rifiutare la dimostrazione.
- La dimostrazione non è intesa con la sua accezione matematica (assoluta) ma probabilistica.

Quindi A è a conoscenza di un segreto s e riesce ad autenticarsi solamente rispondendo correttamente a delle interrogazioni casuali (sfide) poste da B.

PROPRIETÀ

Un protocollo ZK deve rispettare le seguenti proprietà:

- **Completezza**: ovvero se dati un utente onesto e un sistema onesto il protocollo ha successo con schiacciante probabilità
- **Validità**:se un utente A che riesce ad autenticarsi è in possesso dei dati (pubblici e privati) che gli consentono di eseguire il protocollo, allora potrà usare quei dati per autenticarsi in utilizzi successivi del protocollo

Date queste condizioni ogni persona che vuole impersonare un utente deve essere a conoscenza del segreto s.

PROPRIETÀ

- **Zero-Knowledge** proprietà: esiste un algoritmo detto di simulazione che permette di calcolare in tempo polinomiale un informazione non legata con la conoscienza
- **Computazionalità**: se un osservatore C non può distinguere tra trasmissioni reali da quelle simulate. Computazionalmente Perfetto se le probabiltà tra transazioni reali e simulate sono identiche.

l' utente non rilascia informazioni utili (non computabili con un algoritmo a tempo polinomiale) al sistema.

VANTAGGI e SVANTAGGI

- ✓ **Riusabilità**: non c' è un abbassamento del livello di sicurezza con il riuso del protocollo, non vengono infatti rilasciate informazioni utili
- ✓ **No Crittografia**: molti protocolli ZK aboliscono l'utilizzo della crittografia abbassando i tempi di escuzione
- ✘ **Alta computazionablilità:** l'efficienza data da questi protocolli è pagata con alti costi di esecuzione e di memoria usata
- ✘ **Assunzioni non dimostrate:** la maggior parte degli algoritmi si basa su regole che, anche se riconosciute, non hanno ancora vere e proprie dimostrazioni (^{xes} fattorizzaione di un numero)

Basi matematiche

- Sia a un intero appartenente a Z_n^* allora a è un quadrato se esiste un x tale che $a = x^2 \bmod n$
- L' insieme dei quadrati in Z_n è denotato con Q_n
- Dato a appartenente a Q_n e x appartenente a Z_n^* se $a = x^2 \bmod n$ allora x è una radice quadrata mod n
- Dato $n=p_1^{e1}\cdot\ldots\cdot p_k^{ek}$ allora per ogni a appartenente a Q_n esistono 2^k radici

FIAT SHAMIR idea

Il protocollo di fiat-shamir si basa sull' ipotesi che trovare la radice quadrata di un numero modulo n sia computazionalmente equivalente a trovare la fattorizzazione di un numero n.

FIAT SHAMIR
setup

a) A sceglie $n = p \cdot q$ dove p e q sono due numeri primi; tiene segreti p e q e pubblica n

b) A seleziona s tale che $(s,n) = 1$ e $1 \leq s \leq n-1$ e lo tiene segreto.

c) A calcola $v = s^2$ e lo pubblica

- Chiave privata s
- Chiave pubblica (n,v)

FIAT SHAMIR protocollo

I seguenti passi vengono eseguiti t volte

1. A sceglie un numero r a caso ($1 \leq r \leq n-1$) e manda a B $x = r^2 \bmod n$
2. B manda ad A un bit e random (sfida)
3. A manda a B $y = rs^e \bmod n$ (risposta)

   (ovvero r per $e=0$ oppure $r \cdot s$ per $e=1$)

- B verifica la risposta di A con l' uguaglianza $y^2 = x \cdot v^e$

  (ovvero verifica se $r^2=x$ per $e=0$ oppure se $(r \cdot s)^2=xs^2$ per $e=1$)

FIAT SHAMIR esempio

$n=55$ $s=_{55}23$ $s^2=_{55}34$

1) $r=31$
   a) A → $x=r^2=26$ → B
   b) B → $e=1$ → A
   c) A → $y=r\cdot s=53$ → A
   d) B verifica che $(r\cdot s)^2= 4 =r^2\cdot s^2$

2) $r=8$
   a) A → $x=r^2=9$ → B
   b) B → $e=0$ → A
   c) A → $y=r=8$ → B
   d) B verifica $x=9=y^2$

FIAT SHAMIR attacco

1° esempio

- Mister X sceglie r ($1 \leq r \leq n-1$)
- Calcola e invia r^2
- Riceve il bit e
  - Se e=0 Mister X sa rispondere essendo a conoscenza di r
  - Se e=1 Mister X non sa rispondere non conoscendo il valore di s e non potendolo calcolare da s^2

FIAT SHAMIR attacco

2° esempio

- Mister X sceglie x ($1 \leq x \leq n-1$)
- Calcola e invia $r^2 = x^2/s^2$
- Riceve il bit e
  - Se $e=0$ Mister X non sa rispondere: $r = x/(\text{sqrt}(s^2))$ ma calcolare la radice di s^2 è proprio l'operazione che non sa risolvere
  - Se $e=1$ Mister X sa rispondere con x infatti $r^2=x^2/s^2$ -> $r^2 \cdot s^2=x^2$ -> $r \cdot s = x$

FIAT SHAMIR
attacco

Quando un utente tenta di autenticarsi senza conoscere la chiave privata potrà rispondere ad una sola delle due domande.

Ad ogni esecuzione dell' algoritmo la sua possibilità di autenticarsi si dimezza: dopo t passi avrà $(1/2)^t$ possibilità di essersi autenticato.

FEIGE FIAT SHAMIR setup

a) A seleziona $n = p \cdot q$ con p e q segreti tali che siano congrui a $3 \bmod 4$

(in questo modo n è un intero di blum, ovvero preso un intero a modulo n questo ha 4 radici e l' inverso di un quadrato è $x^{((p-1)(q-1)+4)/8}$)

a) k e t sono i due parametri di sicurezza

b) A seleziona k interi $s_1, s_2 \ldots, s_k$ tali che $1 \leq s_i \leq n-1$ e tali che $(n, s_i)=1$ e k random bit b_i

c) A calcola $v_i = (-1)^{bi}(s_i^2)^{-1} \bmod n$ con $1 \leq i \leq k$

La chiave pubblica di A è $(v_1, \ldots v_k; n)$ quella privata $(s_1, \ldots, s_k)$

FEIGE FIAT SHAMIR protocollo

I passi vengono eseguiti t volte

1) A manda a B $x = (-1)^b r^2 \bmod n$ dove r è un intero ($1 \leq r \leq n-1$) e b un bit scelti a caso
2) B manda ad A un vettore di k bit casuali $(e_1,\ldots,e_k)$
3) A manda a B $y = r \cdot \Pi^k_{J=1} s_J^{ej} \bmod n$ (il prodotto tra r e tutti gli s_i selezionati dai bit e_i posti a 1)
4) B calcola $z = y^2 \cdot \Pi^k_{J=1} v_J^{ej} \bmod n$ e verifica che $z=\pm x$ e $z \mathrel{!}= 0$ (ovvero calcola r^2 per tutti i v_i selezionati dai bit e_i posti a 1)

FEIGE FIAT SHAMIR attacco

Quando un utente tenta di autenticarsi senza conoscere la chiave privata avrà una possibilità di autenticarsi pari a $(1/2)^{kt}$
Dove k è la cardinalità della chiave privata di un utente e t il numero di iterazioni del protocollo

ALTRI PROTOCOLLI

- Guillou-Quisquater (estensione di Fiat-Shamir con riduzione del numero di messaggi scambiati e della memoria occupata)
- Schnorr (utilizzo del logaritmo discreto)