Avversari e Scenari di Attacco

Riccardo Longo

Valutare la Sicurezza

- Come si valuta la sicurezza di un cifrario/protocollo?
- Va valutato come viene usato e cosa può andare storto
- Si formalizzano scenario ed attori

Formalizzazione

- Si definiscono le parti coinvolte (attori)
- Si definiscono le azioni possibili
- Si definiscono i requisiti di funzionalità
- Si definiscono i requisiti di sicurezza

Ipotesi e realtà

- Per poter studiare la sicurezza bisogna semplificare
- Si fanno ipotesi ed assunzioni
- La realtà è più complessa
- Bisogna stare attenti a rimanere realistici

Chi partecipa: gli attori

- La prima cosa da definire sono le parti coinvolte
- Utenti legittimi
- Avversari
- Intermediari ed altri

Utenti

- Normalmente si ha un qualche tipo di comunicazione
- Due utenti principali: Mittente e Destinatario
- Nomi classici: **Alice** (A) e **Bob** (B)
- Se ci sono più partecipanti: **Carol** (C), **Dave** (D), ...

Avversari

- Spione, avversario passivo (**Eve**)
- Manipolatore, avversario attivo (**Mallory** o **Trudy**)
- Informatore, infiltrato (**Wendy**)

Intermediari

- Arbitro neutrale o autorità esterna (**Trent**)
- Dimostratore e verificatore (**Peggy** e **Victor**)
- ISP (**Isaac**)
- Persona (o macchina) fidata (**Faith**)
- Guardiano a protezione degli utenti (**Walter**)

Umani e Macchine

- I nomi possono aiutare a descrivere e capire le interazioni
- Spesso gli attori non sono umani ma processi automatizzati
- Umani e macchine hanno caratteristiche e *debolezze* diverse
- Ricordarsi che un modello semplifica la realtà

Forza di uno Scenario di Attacco

- Non tutti i cifrari/protocolli hanno o devono avere la stessa sicurezza
- Alcuni scenari non sono confrontabili per le caratteristiche intrinseche dei cifrari/protocolli
- In generale **meno limitazioni** nello scenario danno più sicurezza
- L'attaccante è più forte quando:
  - ha **più risorse** (memoria, potenza di calcolo)
  - **interagisce di più** (può fare più cose)
  - ha un **obiettivo più facile**
- Più forte è l'attaccante, più forte è lo scenario, **maggiore è la sicurezza**

Obiettivi di un Attaccante

- Ricavare la chiave di cifratura
- Leggere un messaggio cifrato
- Distinguere quale tra due messaggi noti è stato cifrato
- Impersonare un utente
- Modificare un messaggio (mantenendone la validità)

Risorse di un Attaccante

- Potenza di calcolo e memoria (limitati/illimitati)
- Capacità di intercettazione/lettura
- Modalità di interazione (*DOS*, *replay*,. . .)
- Oracoli (cifratura, decifratura, . . .)
- **Side Channel** (memory leak, power analysis, frequency analysis,. . .)

Scenari Classici: Risorse e Interazioni

- **Ciphertext Only**: l'attaccante vede solo un certo numero di cifrati
- **Known Plaintext**: è noto un certo numero di coppie [messaggio, cifrato]
- **Chosen Plaintext**: l'attaccante ha facoltà di scegliere un certo numero di messaggi di cui ottenere il cifrato
- **Chosen Ciphertext**: si può ottenere la decifratura di un certo numero di cifrati

Scenari Classici: Obiettivi

- **Key Recovery**: l'attaccante deve ricostruire la chiave usata
- **Plaintext Recovery**: ricostruire il messaggio in chiaro corrispondente ad un cifrato (che non era già conosciuto)
- **Distinguisher**: dato un cifrato l'attaccante deve riuscire a distinguere tra due alternative:
  - quale tra due messaggi noti è il plaintext corrispondente
  - è un vero cifrato o una sequenza random
  - appartenenza della chiave ad una specifica classe
  - ...

Assunzioni e Dimostrazioni

L'ideale è dimostrare matematicamente che un certo schema è sicuro

- Si formalizza lo schema (attori, interazioni, obiettivi)
- Si formulano assunzioni:
  - capacità e limiti degli attori
  - proprietà del sistema (canali di comunicazione,...)
  - risolvibilità di alcuni problemi matematici
- Si dimostra che se l'attaccante ha successo viene violata un'assunzione

Limiti della Teoria

La realtà può discostarsi dal modello in molti modi:

- **attori** non previsti
- **azioni** diverse
- altri **obiettivi**
- le **proprietà del sistema** non coincidono
- **capacità** non considerate

Esempio: il protocollo WPA2 ha una dimostrazione di sicurezza, ma ci sono attacchi che aggirano il modello.

Esempio: semplice comunicazione

Attori:

- Mittente
- Destinatario
- Avversario

Requisiti di Funzionalità:

- Il destinatario viene a conoscenza del contenuto del messaggio
- Comunicazione asincrona

Requisiti di Sicurezza:

- La probabilità che l'avversario venga a conoscenza del contenuto del messaggio è minore di ε

Prima soluzione: Dead Drop

"Protocollo":

- Mittente e destinatario si accordano su un punto di scambio segreto in modo che sia noto solo a loro
- Il mittente lascia un biglietto col messaggio nel punto prestabilito
- Il destinatario recupera il biglietto e legge il messaggio

Dead Drop: ipotesi

Ipotesi di Funzionalità:

a. Il mittente può trasferire ogni possibile messaggio su un biglietto
b. Il destinatario può correttamente recuperare ogni possibile messaggio da un biglietto
c. I possibili punti di scambio sono accessibili
d. I possibili punti di scambio possono ospitare un biglietto in modo che resti integro e recuperabile

Ipotesi di Sicurezza:

1. I possibili messaggi sono più di $\frac{1}{\varepsilon}$ e tutti equiprobabili
2. I possibili punti di scambio sono N e tutti equiprobabili
3. Ci vogliono m minuti per controllare se c'è un biglietto in un punto di scambio
4. L'avversario ha meno di k minuti per fare l'attacco
5. Vale la disequazione: $\frac{k}{mN} < \varepsilon$

Dead Drop: analisi di funzionalità

Dimostrazione.

- Grazie all'ipotesi a il mittente riesce a preparare il biglietto col messaggio
- Grazie alle ipotesi c e d il mittente riesce ad arrivare al punto prestabilito e lasciarvi il biglietto
- Grazie alle ipotesi c e d il destinatario riesce ad arrivare al punto prestabilito e recuperare il biglietto integro
- Grazie all'ipotesi b il destinatario riesce a recuperare il messaggio corretto dal biglietto.

□

Dead Drop: analisi di sicurezza

Dimostrazione.

- Grazie all'ipotesi 1 la probabilità che l'avversario indovini il messaggio senza trovare il biglietto è $< \varepsilon$
- Grazie alle ipotesi 3 e 4 l'avversario riesce a controllare al più $\frac{k}{m}$ punti di scambio
- Grazie all'ipotesi 2 la probabilità che l'avversario trovi il punto di scambio giusto con t tentativi a disposizione è $\frac{t}{N}$
- Grazie alle precedenti osservazioni e all'ipotesi 5 la probabilità che l'avversario riesca a recuperare il biglietto è $< \varepsilon$

Seconda soluzione: Cassetta di Sicurezza

"Protocollo":

- Mittente e destinatario hanno le uniche due chiavi che aprono una cassetta di sicurezza
- Il mittente lascia un biglietto col messaggio nella cassetta
- Il destinatario recupera il biglietto e legge il messaggio

Cassetta di Sicurezza: ipotesi

Ipotesi di Funzionalità:

Stesse ipotesi a e b su messaggi e biglietti

c. La cassetta è accessibile

d. La cassetta può ospitare un biglietto in modo che resti integro e recuperabile

Ipotesi di Sicurezza:

1. Stessa ipotesi 1 sui messaggi
2. La probabilità che la cassetta si riesca ad aprire senza una delle due chiavi è $< \varepsilon$
3. La probabilità che un attore diverso da mittente e destinatario riesca ad ottenere una delle due chiavi è $< \varepsilon$

Cassetta di Sicurezza: analisi di funzionalità

Dimostrazione.

- Grazie all'ipotesi a il mittente riesce a preparare il biglietto col messaggio
- Grazie alle ipotesi c e d il mittente riesce ad arrivare allla cassetta e lasciarvi il biglietto
- Grazie alle ipotesi c e d il destinatario riesce ad arrivare alla cassetta e recuperare il biglietto integro
- Grazie all'ipotesi b il destinatario riesce a recuperare il messaggio corretto dal biglietto

□

Cassetta di Sicurezza: analisi di sicurezza

Dimostrazione.

- Grazie all'ipotesi 1 la probabilità che l'avversario indovini il messaggio senza avere il biglietto è $< \varepsilon$
- Grazie alle ipotesi 2 e 3 la probabilità che l'avversario riesca a recuperare il biglietto dalla cassetta è $< \varepsilon$

□

Questo protocollo può essere considerato più sicuro perché abbiamo indebolito le ipotesi di sicurezza, in particolare tolto il limite alla durata dell'attacco.
Notare però che le ipotesi sulla cassetta possono diventare irrealistiche o più forti delle precedenti, in tal caso il protocollo non è "più sicuro".