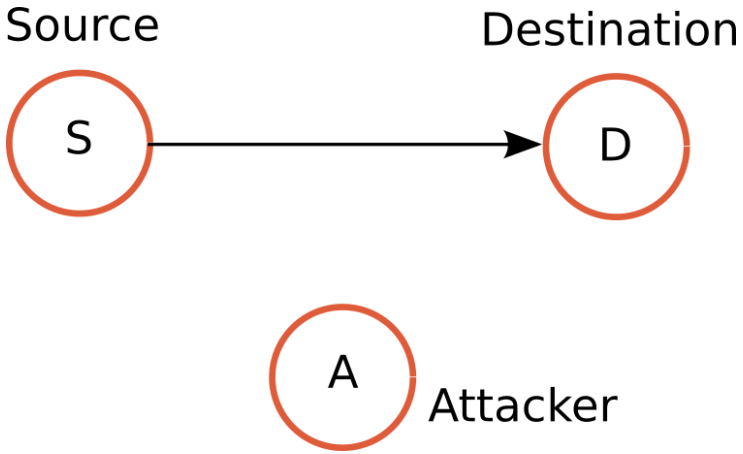
Attacchi alla Confidenzialità, Integrità e Disponibilità

Indice

- Impatto degli attacchi alla CIA
- Cenni sui rimedi

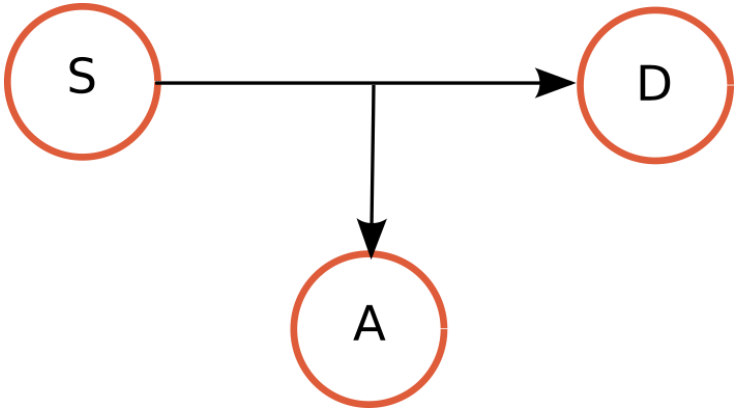
Classi di attacchi

- L'informazione (o un servizio) si muove da una sorgente a una destinazione
- L'attaccante potrebbe **sovvertire** questo schema in diversi modi



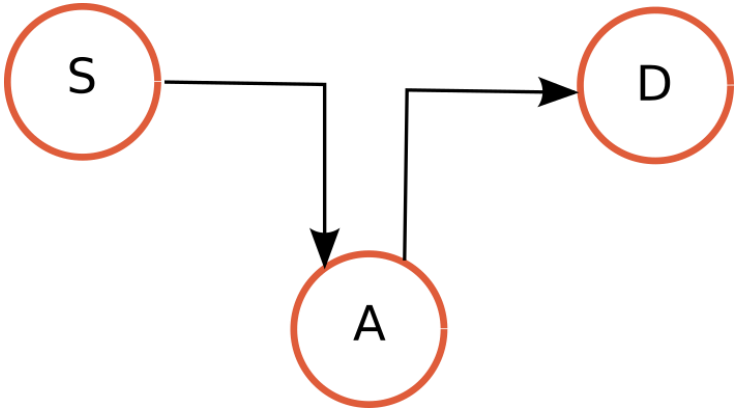
Furto (Stealing)

- L'attaccante ottiene **accesso non autorizzato** all'informazione
- La **confidenzialità** viene meno
- Esempi:
  - S è un database vulnerabile
  - S manda un numero di carta di credito a D "in chiaro"



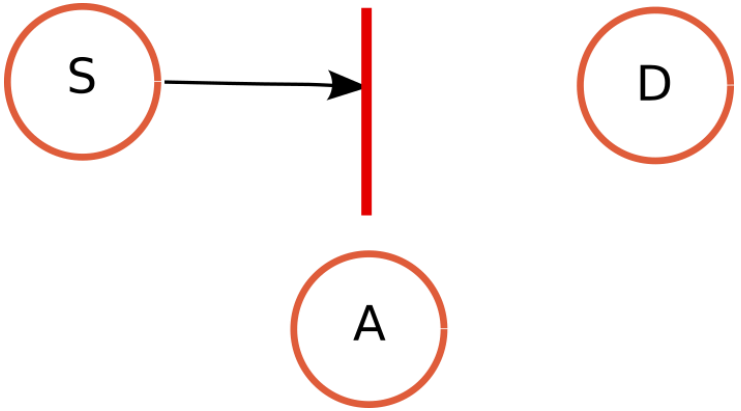
Corruzione (Corrupting)

- L'attaccante **modifica in modo malevolo** l'informazione
- L'**integrità** viene meno
- Esempi:
  - A redirige un trasferimento bancario partito da S
  - NOTA: A può trovarsi nel browser o nel mezzo dell'infrastruttura di comunicazione (*Man-in-the-middle*)



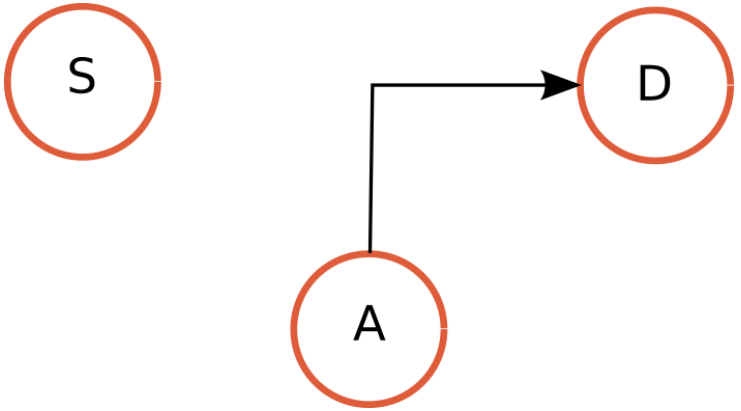
Inibizione (Inhibiting)

- L'attaccante **stoppa** il flusso di informazione
- La **disponibilità (availability)** viene meno
- Esempi:
  - DoS su un sistema di voto elettronico o un sito
  - DoS sulla rete elettrica (e.g., attacchi in Ucraina)



Contraffazione (Forging)

- L'attaccante **crea nuova informazione**
- L'**autenticità** viene meno (così come la **credibilità**)
- Esempi:
  - Falsificare una firma attraverso una vulnerabilità crittografica (e.g., le collisioni presenti nel protocollo di hashing)



Attacchi ai messaggi in transito

- I messaggi che transitano sulla rete possono essere passibili di diversi tipi di attacco, come riassunto nelle slide seguenti

Attacchi ai messaggi in transito

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. Ripudio della sorgente
8. Ripudio della destinazione

Attacchi ai messaggi in transito

1. ***Disclosure***
2. Traffic analysis
3. Masquerade
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. Ripudio della sorgente
8. Ripudio della destinazione

- Il messaggio cifrato è letto da soggetti che non possiedono la chiave (cause: algoritmo di cifratura debole o chiave debole)

Attacchi ai messaggi in transito

1. Disclosure
2. ***Traffic analysis***
3. Masquerade
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. Ripudio della sorgente
8. Ripudio della destinazione

- L'analisi del numero e della frequenza dei messaggi può fornire informazioni all'attaccante sul tipo di interazione tra due soggetti su rete

Attacchi ai messaggi in transito

1. Disclosure
2. Traffic analysis
3. ***Masquerade***
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. Ripudio della sorgente
8. Ripudio della destinazione

- Possono essere immessi sulla rete messaggi da fonti malevoli per ingannare un soggetto sulla rete

Attacchi ai messaggi in transito

1. Disclosure
2. Traffic analysis
3. Masquerade
4. ***Modifica del contenuto***
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. Ripudio della sorgente
8. Ripudio della destinazione

- Il contenuto di un messaggio può essere modificato

Attacchi ai messaggi in transito

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Modifica del contenuto
5. ***Modifica della sequenza dei messaggi***
6. Modificazione della tempistica
7. Ripudio della sorgente
8. Ripudio della destinazione

- Una sequenza di invio può venir alterata da un attaccante in modo che i messaggi giungano a destinazione in ordine diverso o senza qualche messaggio

Attacchi ai messaggi in transito

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. ***Modificazione della tempistica***
7. Ripudio della sorgente
8. Ripudio della destinazione

- La sequenza dei messaggi o il singolo messaggio possono venir ritardati.

Attacchi ai messaggi in transito

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. ***Ripudio della sorgente***
8. Ripudio della destinazione

- La sorgente (malevola) può negare di aver inviato certi messaggi

Attacchi ai messaggi in transito

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. Ripudio della sorgente
8. ***Ripudio della destinazione***

- Il ricevente può negare di aver ricevuto certi messaggi

Analisi degli attacchi

1. ***Disclosure***
2. ***Traffic analysis***
3. Masquerade
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. Ripudio della sorgente
8. Ripudio della destinazione

- Questi due attacchi riguardano la **confidenzialità** del messaggio e possono essere risolti con gli algoritmi di cifratura e con steganografia che vedremo tra poco

Analisi degli attacchi /2

1. Disclosure
2. Traffic analysis
3. ***Masquerade***
4. ***Modifica del contenuto***
5. ***Modifica della sequenza dei messaggi***
6. ***Modificazione della tempistica***
7. Ripudio della sorgente
8. Ripudio della destinazione

- Questi attacchi possono essere mitigati con l'autenticazione del messaggio (MAC) che vedrete

Analisi degli attacchi /3

1. Disclosure
2. Traffic analysis
3. Masquerade
4. Modifica del contenuto
5. Modifica della sequenza dei messaggi
6. Modificazione della tempistica
7. ***Ripudio della sorgente***
8. ***Ripudio della destinazione***

- Questi attacchi possono essere mitigati tramite le firme digitali.

Analisi degli attacchi /4

Autenticare un messaggio vuol dire

- riuscire a dedurre con una probabilità molto altra che il messaggio ricevuto proviene davvero da una certa fonte.
- capire se il messaggio è effettivamente quello originariamente spedito dalla fonte, senza essere modificato.

I protocolli per l'autenticazione del messaggio devono permettere di accorgersi di eventuali modifiche.

Rimedi

- Per resistere agli attaccanti e agli attacchi occorre avere a disposizione delle soluzioni – CIA - che garantiscano confidenzialità, integrità e autenticazione nelle comunicazioni che si scambiano due o più parti che comunicano su una rete insicura.
- Tali soluzioni sono la crittografia (a chiave simmetrica e asimmetrica), la steganografia, gli hash crittografici, e i protocolli costruiti su di esse.

Rimedi /2

- La confidenzialità viene garantita da
  - Crittografia: algoritmi di cifratura che trasformano un testo in chiaro in un testo cifrato che comprensibile solo da quelli che hanno una chiave per decifrarlo
  - Steganografia: Tecniche per nascondere messaggi in messaggi apparentemente innocui
- L'integrità viene garantita attraverso l'uso di funzioni hash crittografiche che permettono di rilevare «manomissioni» di un messaggio in transito su una rete insicura.
- L'autenticazione viene invece ottenuta combinando tecniche crittografiche e hash.