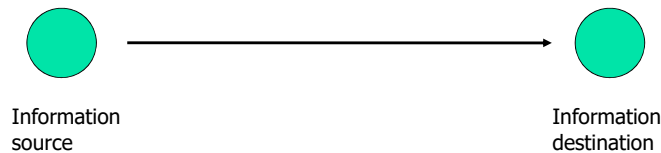


## Concetti Basilari

## Architettura di Riferimento

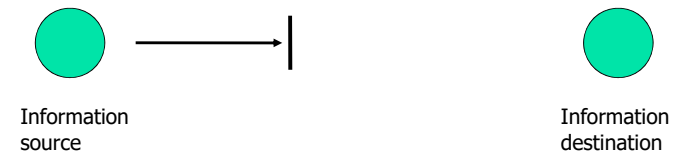
- Ci uniformeremo alla OSI Security Architecture
- Descrive:
  - **Attack** – azione che compromette la sicurezza delle informazioni di un'organizzazione
  - **Mechanisms** – individuano o prevengono un attacco o ristabiliscono la situazione precedente un attacco
  - **Services** – migliorano la sicurezza dei sistemi

## Security Attacks (1)



Normal Flow

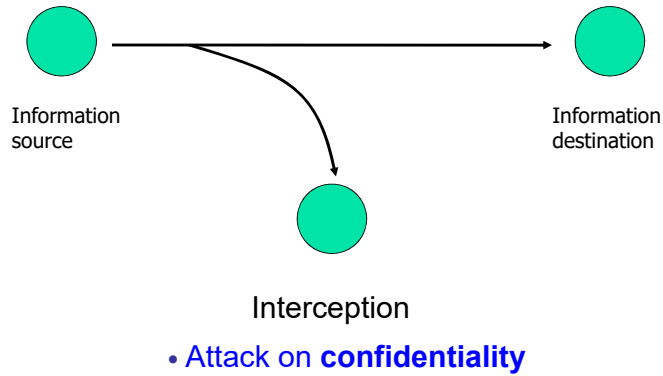
## Security Attacks (2)



Interruption

- **Attack on availability**

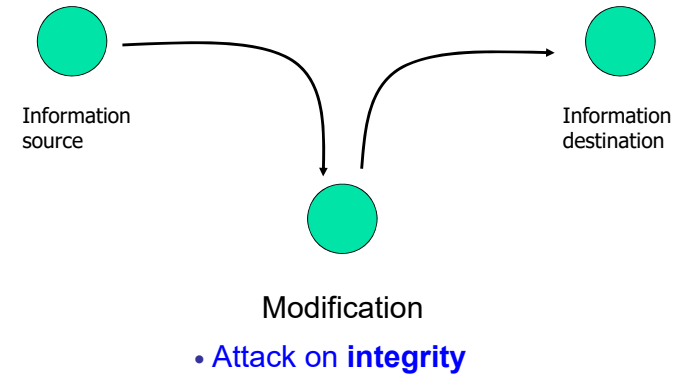
## Security Attacks (3)



Concetti Basilari

5

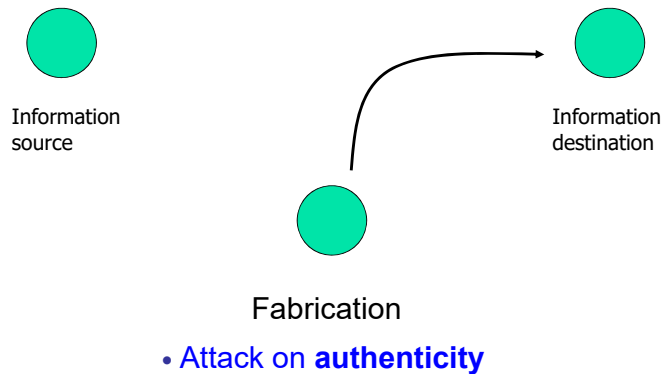
## Security Attacks (4)



Concetti Basilari

6

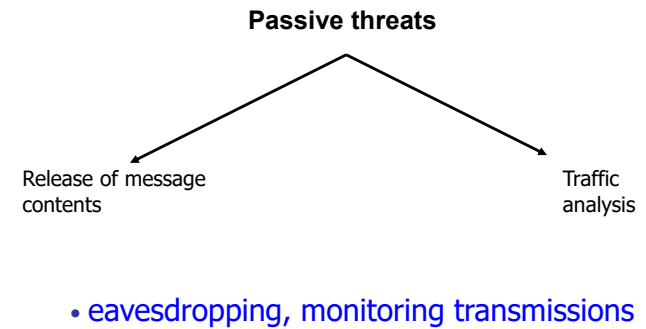
## Security Attacks (5)



Concetti Basilari

7

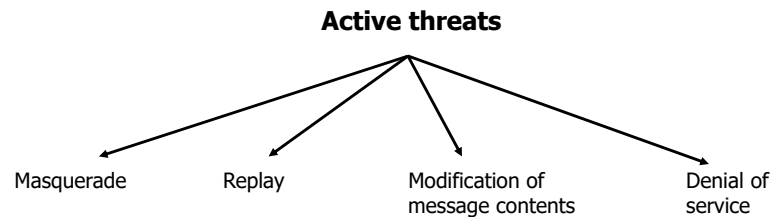
## Security Attacks (6)



Concetti Basilari

8

## Security Attacks (7)



- some modification of the data stream

## Security Services (1)

- **Confidentiality** – protezione da attacchi passivi
- **Authentication** – sei chi dici di essere
- **Integrity** – ricevuto come inviato, senza modifiche, aggiunte, cancellazioni

## Security Services (2)

- **Nonrepudiation** – impossibilità di negare l'invio/ricezione di un messaggio
- **Access Control** – capacità di limitare / controllare gli accessi al sistema
- **Availability** – garanzia dagli attacchi mirati a ridurre o limitare la disponibilità del sistema

## Security Mechanisms (1)

- Meccanismi Specifici (livello protocolli OSI):
  - **Cifratura** dei messaggi mediante crittografia
  - **Firma digitale** dati aggiunti al messaggio per dimostrare l'autenticità della sorgente
  - **Controllo degli accessi**: definizione dei diritti di accesso alle risorse
  - **Integrità dei dati**, sia singolo pck che un flusso
  - **Scambio di autenticazioni**, scambio di info per autenticazione reciproca
  - **Traffico di riempimento**: inserimento di bit nei vuoti di un flusso, per limitare l'analisi del traffico
  - **Controllo del routing**: definizione della route da seguire
  - **Certificazione**: uso di terza parte fidata

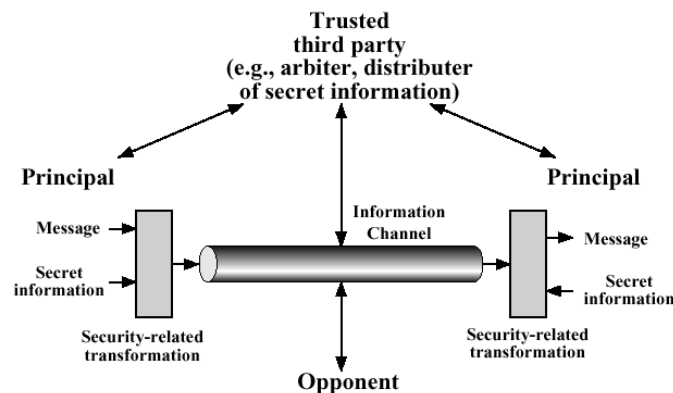
## Security Mechanisms (2)

- Meccanismi Pervasivi (indipendenti dai protocolli OSI):
  - **Funzionalità fidate**: insieme di caratteristiche e criteri che permettono di percepire una comunicazione come sicura
  - **Etichette di sicurezza**: marcatura di attributi di sicurezza
  - **Individuazione degli eventi** rilevanti per la sicurezza
  - **Prove** di verifica di sicurezza
  - **Recupero** di sicurezza

## Servizi vs Meccanismi

	Cifrat ura	Firma Digitale	Controllo Accessi	Integrità Dati	Scambio Autentic.	Traffico Riemp.	Controllo Routing	Certificaz ione
Autenticazio ne Entità Paritaria	OK	OK			OK			
Autent. Origine dati	OK	OK						
Controllo Accessi			OK					
Riservatezza	OK						OK	
Riservatezza Flusso Traffico	OK					OK	OK	
Integrità Dati	OK	OK		OK				
Non ripudio		OK		OK				OK
Disponibilità				OK	OK			

## Network Security Model (1)



## Network Security Model (2)

- La progettazione di un servizio di sicurezza necessita delle seguenti attività
  - **Progettazione** dell'algoritmo
  - **Generazione** delle informazioni segrete da usare
  - Sviluppo di metodi per **distribuire e condividere** le informazioni
  - Specifica del **protocollo** usato dai partecipanti