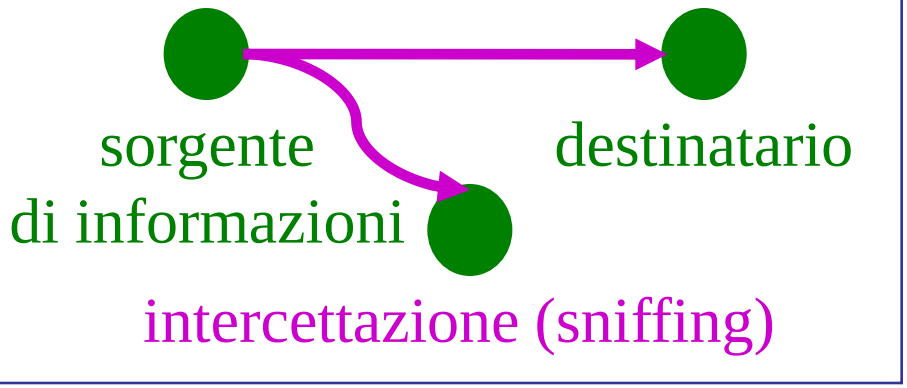
sicurezza delle reti
livelli 1-2

attacchi nelle reti

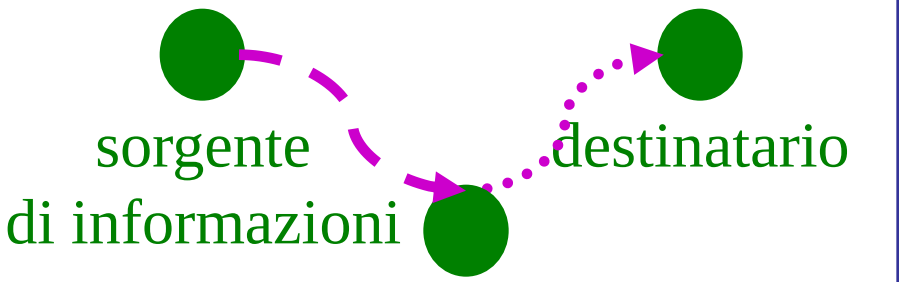
flusso normale

interruzione (DoS)

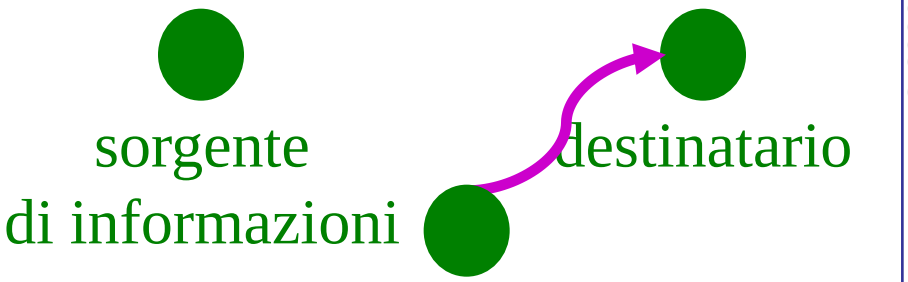


intercettazione (sniffing)

intercettazione (MiM passivo)

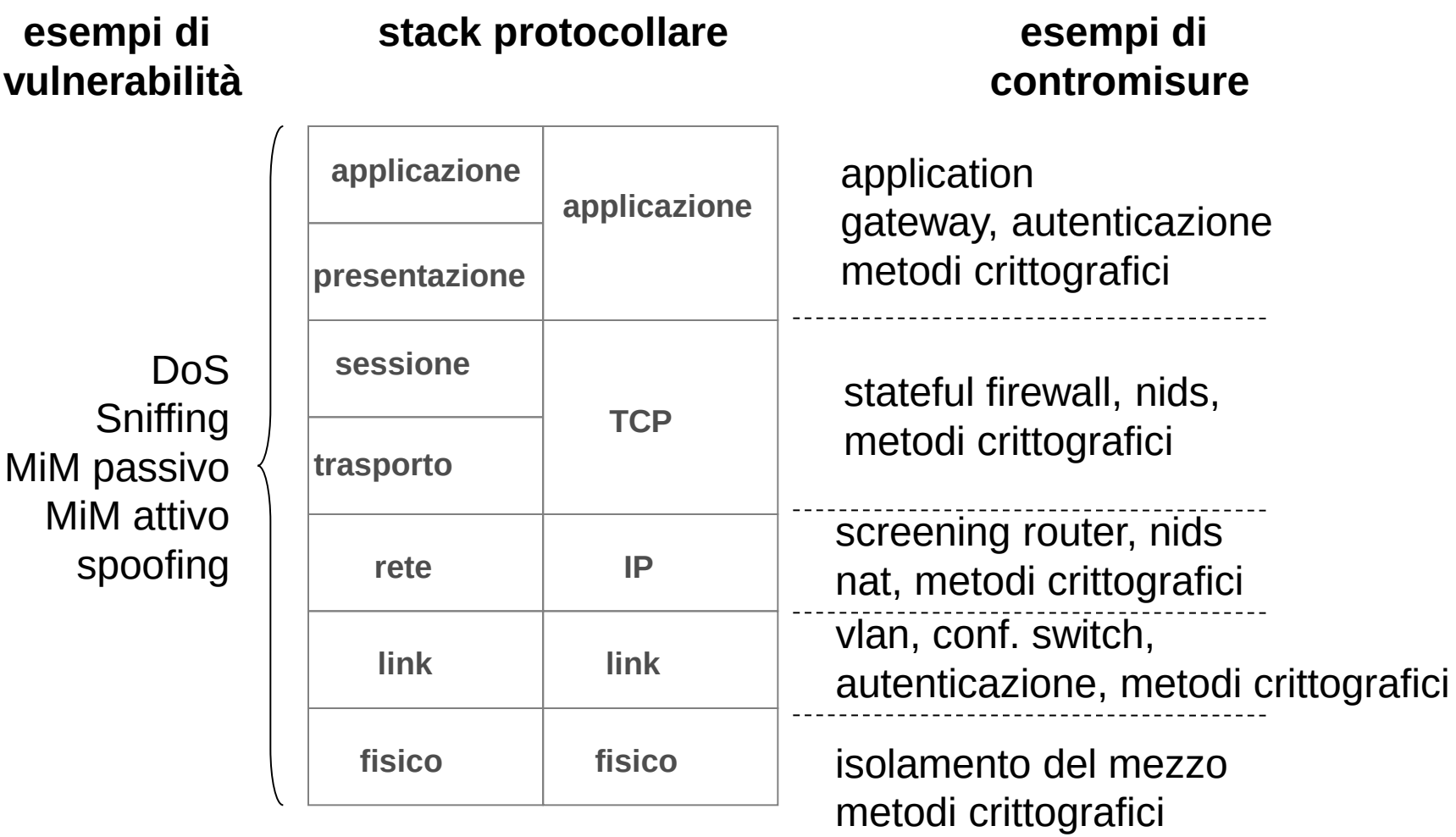


modifica (MiM attivo)



creazione (spoofing)

la sicurezza nelle reti



confinamento nelle reti

- il traffico è (o dovrebbe essere) ammesso solo tra sistemi e/o utenti con caratteristiche di sicurezza analoghe (principio di isolamento)
- esempi di classi di utenti
  - amministrazione
    - integrità e disponibilità: critiche per il business
    - confidenzialità: ciritica per legge
    - insieme di applicazioni ben definito
    - sistemi sotto controllo diretto
  - docenti
    - integrità e disponibilità: critiche per il business
    - confidenzialità: ciritica per certi aspetti particolari
    - richiesta alta flessibilità nelle applicazioni
    - il controllo dei sistemi è delegato ai gruppi di ricerca
  - studenti
    - best effort
    - sistemi non controllabili
  - utenti da internet di ricerca
    - servizi selezionati: web, email, siti di ricerca interni, login alle macchine di ricerca e a utenti da internet (altri)
    - servizi selezionati: web, email, siti di ricerca interni

sicurezza del mezzo trasmissivo

- cavi in rame
  - vulnerabilità
    - wiretapping
    - taglio
    - emissione elettromagnetica
  - contromisure
    - protezione fisica
    - wiretapping detection
- fibra
  - vulnerabilità
    - wiretapping
    - taglio
  - contromisure
    - protezione fisica
    - wiretapping detection (metodi quantistici, l'osservatore non può non modificare certe caratteristiche fisiche del segnale)

sicurezza del mezzo trasmissivo

- wireless
  - vulnerabilità
    - copertura “ad area” non “a presa”
      - impossibile controllare chi riceve il traffico
    - area di copertura varia con la sensibilità delle stazioni
      - antenne fortemente direzionali possono interagire con hot spot molto lontani
    - facile avere utenti “parassiti”
    - DoS elettromagnetico (*jamming*)
      - non adatto a sistemi la cui disponibilità è critica
    - banda limitata
      - tanto più limitata quanto più resiliente a jamming (uso di error correction codes)
  - contromisure
    - confidenzialità e integrità: meccanismi crittografici a livello data link (più o meno efficaci)

livello data link

switch

- vulnerabilità
  - mac address spoofing/flooding
    - impatto su arp, spanning tree, e livelli superiori
  - e altri problemi mitigabili: bugs del firmware, errori di configurazione
- contromisure
  - switch sofisticati permettono di rilevare e contrastare attacchi basati su mac address spoofing
    - es. tracciando le porte dove appare un mac address
  - autenticazione
    - mac address lock (protezione blanda)
    - web based (captive portal)
      - al primo accesso funziona solo dhcp e dns
      - lo switch fa da web server e tramite http chiede username e password
    - 802.1X (vedi dopo)
  - isolamento
    - VLAN
      - vulnerabilità: GVRP è abilitato di default per standard e permette la configurazione automatica di vlan, oramai obsoleto e deletereo.

virtual lan vs. real lan

- le “forze” che guidano il progetto della rete fisica e delle vlan sono diverse
- rete fisica, cioè switch e cablaggio
  - ha come obiettivo la rete economicamente più conveniente che soddisfi i seguenti vincoli
    - piena connettività tra le prese
    - prestazioni richieste
    - vincoli ambientali (es. posizione spazi adibiti agli impianti)
    - vincoli tecnologici (es. lunghezza dei cavi)
    - normative (es. materiali non infiammabili)
    - affidabilità (se richiesta, es. resiste al fault di uno switch)
- vlan, cioè configurazione ideale “desiderata”
  - ha come obiettivo la migliore configurazione che soddisfi…
    - le specifiche funzionali
      - chi deve essere connesso con chi? vedi strutture organizzative che occupano l’edificio (es. dipartimenti, reparti, ecc)
    - le specifiche di sicurezza basate sulle classi di utenti (vedi isolamento)
    - facilità di gestione (es. ciascuna vlan un amministratore)

vlan

- su un singolo switch
  - ciascuna porta è associata ad una vlan
  - uno “switch virtuale“ per ciascuna vlan
- su più switch: 802.1Q
  - tra uno switch e l’altro i pacchetti viaggiano taggati con l’identificatore della vlan (802.1p)
- comportamenti caratteristici
  - confinamento di broadcast e unicast
    - switch di scarsa qualità (non standard) confinavano solo il broadcast (vulnerabile)
  - la comunicazione tra vlan deve avvenire attraverso un router proprio come tra lan distinte
- argomenti correlati
  - vlan asimmetriche, vlan per protocollo, GVRP, multiple spanning tree

Wi-Fi

- autenticazione
  - web based (captive portal)
    - al primo accesso funziona solo dhcp e dns
    - lo switch fa da web server e tramite http chiede username e password
  - 802.1X
  - in ogni caso basati su metodi crittografici
- isolamento (sia per confidenzialità che per integrità) assicurato solo con metodi crittografici
  - vedi parte di applicazioni crittografiche