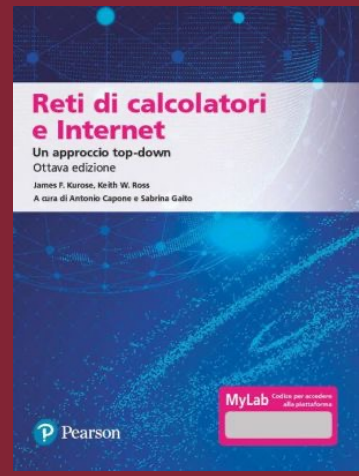
Reti di Elaboratori

Sicurezza



SAPIENZA
UNIVERSITÀ DI ROMA

Alessandro Checco
alessandro.checco@uniroma1.it

Capitolo 1

Capitolo 1: sommario

- Cos'è *Internet* ?
- Cos'è *un* protocollo?
- Periferia della rete: host, rete di accesso, supporti fisici
- Nucleo di rete: commutazione pacchetto/circuito, struttura internet
- Prestazioni: loss, delay, throughput
- Sicurezza
- Livelli di protocollo, modelli di servizio
- Storia

Modello OSI

Due livelli non trovati nello stack del protocollo Internet!

- *presentazione:* consentire alle applicazioni di interpretare il significato dei dati, ad esempio crittografia, compressione, convenzioni specifiche della macchina
- *sessione:* sincronizzazione, checkpoint, ripristino dello scambio di dati
- Lo stack protocollare Internet non ha questi livelli!
  - questi servizi, *se necessari,* devono essere implementati nell'applicazione
  - è necessario?

I sette layer OSI/ISO reference model

Sicurezza della rete

- campo della sicurezza della rete
  - come i malintenzionati possono attaccare le reti di computer
  - come possiamo difendere le reti dagli attacchi
  - come progettare architetture immuni agli attacchi
- Internet non originariamente progettato pensando alla sicurezza
  - *visione originale:* “un gruppo di utenti che si fidano reciprocamente collegati a una rete trasparente” ☺
  - I progettisti di protocolli Internet devono correre ai ripari e costruire soluzioni che complementano questa visione originale
  - considerazioni sulla sicurezza a tutti i livelli dello stack!

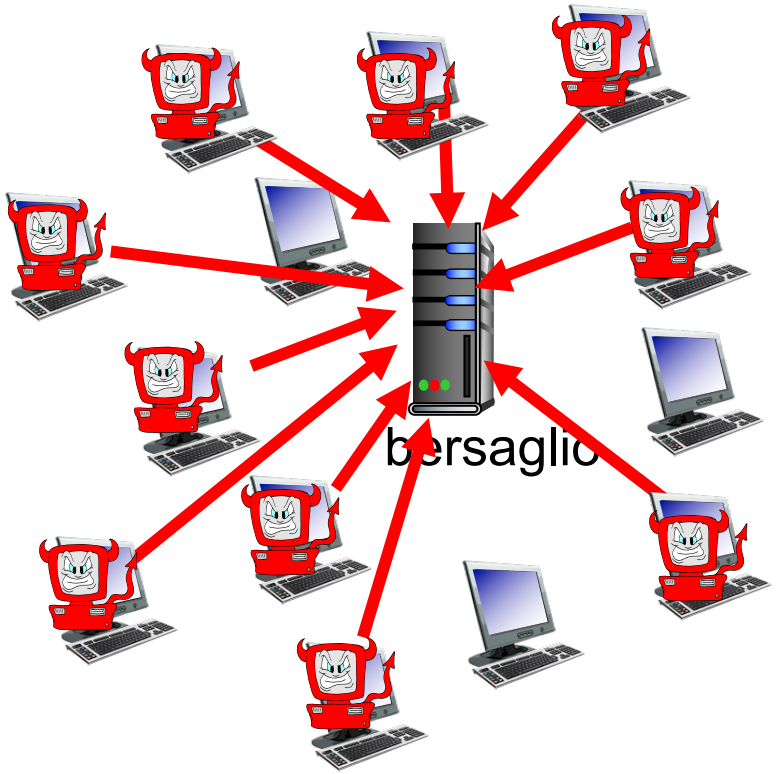
Attacchi alla rete: malware

- il malware può entrare nell'host tramite:
  - *virus:* infezione autoreplicante mediante la ricezione/esecuzione di oggetti (ad es. allegati di posta elettronica)
  - *worm:* infezione autoreplicante che viene eseguito passivamente alla ricezione di un oggetto
- malware spyware può registrare sequenze di tasti, siti Web visitati, caricare informazioni sul sito di raccolta
- l'host infetto può diventare parte di una botnet, utilizzato per spam o attacchi DDoS (Distributed Denial of Service)

Attacchi alla rete: denial of service

Denial of Service (DoS): l'attaccante rende le risorse (server, larghezza di banda) non disponibili al traffico legittimo sovraccaricando la risorsa con traffico fasullo

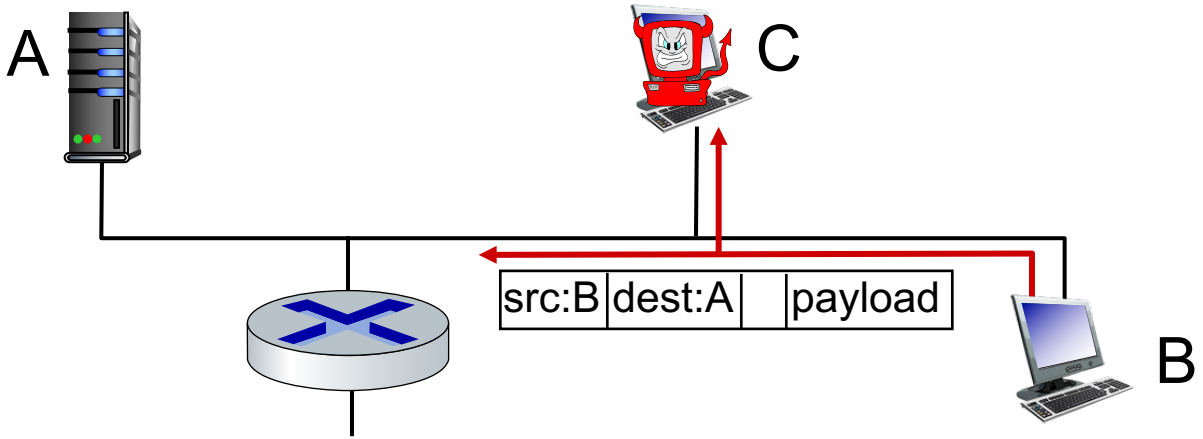
1. seleziona il bersaglio
2. irrompere negli host della rete (ad es. con una botnet)
3. inviare pacchetti al bersaglio da host compromessi



Attacchi alla rete: intercettazione di pacchetti

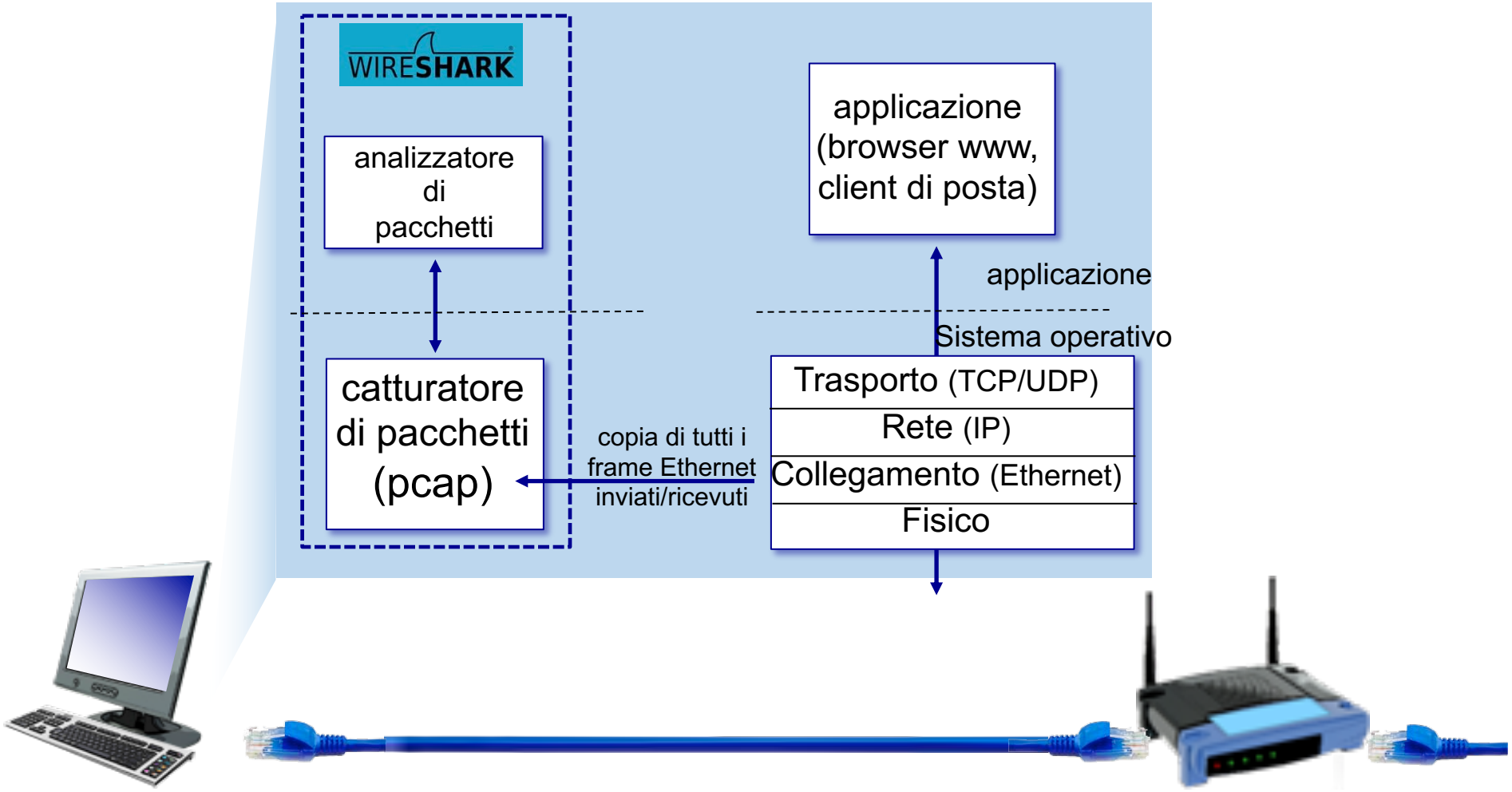
packet "sniffing"

- spesso via mezzi di trasmissione (Ethernet condivisa, wireless)
  - In alcuni casi tramite switch compromessi (ad es. attacchi governativi)
- l'interfaccia di rete malevola legge/registra tutti i pacchetti (ad esempio, comprese le password!) che passano



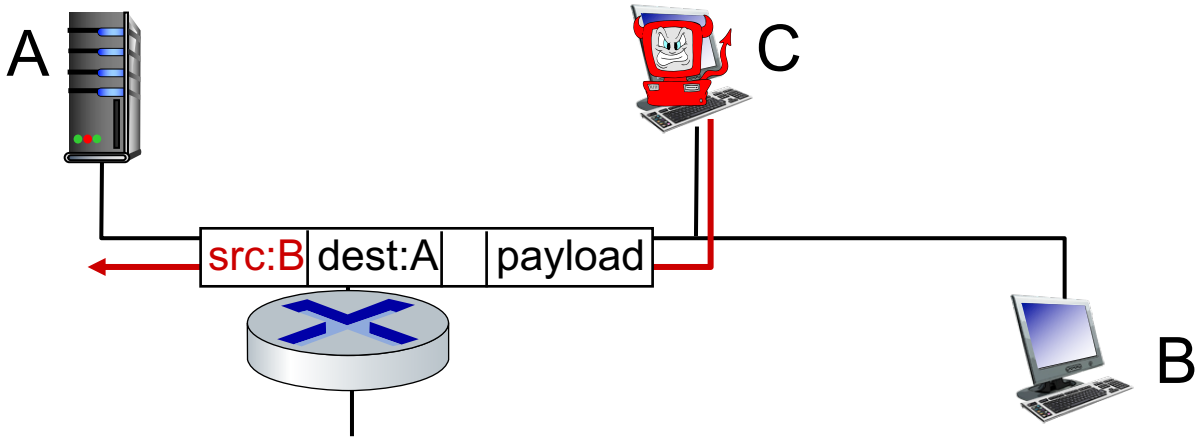
Il software Wireshark è uno sniffer di pacchetti (gratuito)

Wireshark


WIRESHARK
analizzatore di pacchetti
catturatore di pacchetti (pcap)
copia di tutti i frame Ethernet inviati/ricevuti
applicazione (browser www, client di posta)
applicazione
Sistema operativo
Trasporto (TCP/UDP)
Rete (IP)
Collegamento (Ethernet)
Fisico

Attacchi alla rete: falsa identità

IP Spoofing: inviare un pacchetto con un indirizzo di origine falso



… molto di più sulla sicurezza nel Capitolo 8 (in Inglese)

Forme di difesa

- **autenticazione**: dimostrare che il destinatario è effettivamente chi dichiara di essere
  - Ad esempio le reti cellulari usano la SIM card
- **confidenzialità**: tramite crittografia
- **controllo integrità del messaggio**: firme digitali per prevenire e riconoscere manomissioni del messaggio
- **restrizioni di accesso**: VPNs protette da password
- **firewalls**: middleboxes specializzate, usate nel nucleo e nell'access network:
  - off-by-default: filtra i pacchetti in arrivo mantenendo soltanto quelli da selezionati destinatari, mittenti, applicazioni
  - riconoscere e reagire agli attacchi DOS