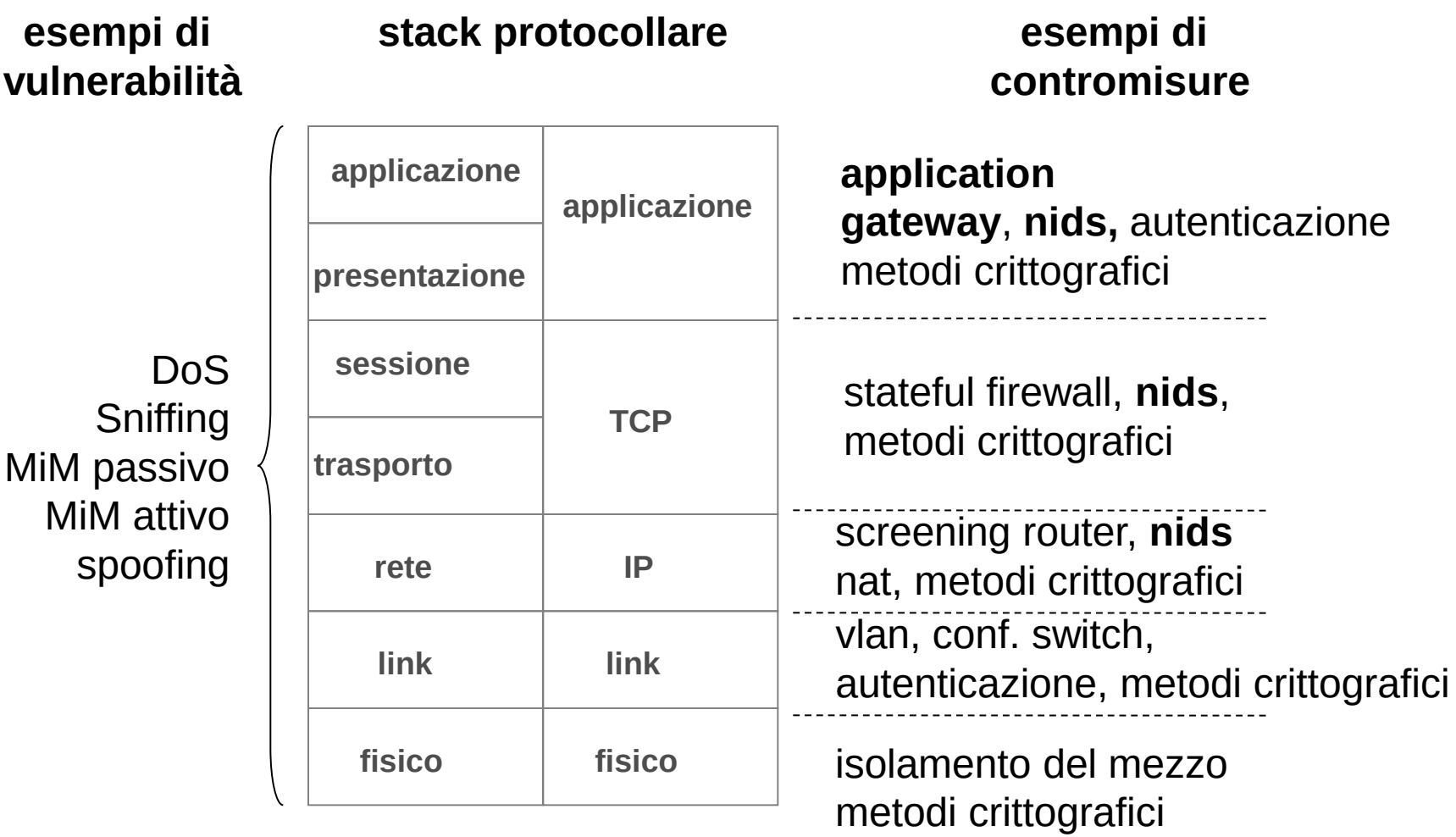
sicurezza di rete a livello applicativo e Network IDS

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

la sicurezza nelle reti



© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

proxy applicativi

- due sessioni di trasporto
  - Client ↔ Proxy ↔ Sever
- permettono verifiche di sicurezza a livello applicativo
  - devono conoscere i protocollo applicativo o almeno parte di esso
- **spesso usati per prevenire comportamenti insicuri degli utenti della intranet**
- protocolli
  - http, https
  - smtp, pop3, imap
  - ftp, dns, sql

- circuit level proxies (SOCKS)
  - proxy generico, indipendente dal protocollo applicativo
  - utile per forzare una autenticazione a livello tcp o udp

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

web proxy: obiettivi

- **autenticazione, controllo di accesso al servizio**
- **test per codice malevolo**
- anonimità
- prestazioni: caching
  - squid
- modifica contenuto
  - censura
  - riformattazione per schermi piccoli (smartphone)
- reverse proxy: un proxy in prossimità di un web server che riceve le richieste da Internet
  - sicurezza, load balancing, encryption acceleration, cache del contenuto statico, autenticazione
  - open source: nginx, treafik

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

transparent web proxy

- un web proxy regolare richiede la configurazione del browser
  - scomodo
  - la presenza del proxy è palese
- un proxy “transparent” intercetta richieste http qualsiasi
  - non richiede configurazione del browser
  - il proxy c’è ma non si vede
- esercizio: configurare linux netfilter per un transparent proxy

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

web proxy: vulnerabilità

- il protocollo http prevede il metodo CONNECT
- tale metodo viene interpretato dai proxy come un comando per lasciare passare connessioni arbitrarie
  - usato per connessioni http criptate
    - https (http su secure socket layer)
  - se connessione è criptata il proxy non può conoscerne il contenuto
- disabilitare CONNECT comporta l'impossibilità di usare https

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

web proxy e SSL/TLS

- nelle grandi organizzazioni è necessario supportare sia SSL/TLS sia una verifica a livello applicativo
- soluzione: le macchine degli utenti hanno un certificato dell'organizzazione installato
  - gli utenti non hanno il controllo amministrativo delle proprie macchine
- il web proxy può fare MitM su session SSL/TLS perché ha la corrispondente chiave privata.

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

Network Intrusion Detection Systems (NIDS)

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

Network IDS (NIDS)

- verifica la presenza sulla rete di traffico riconducibile ad attività sospette
- elementi
  - sniffer
    - particolari precauzioni per reti switched
  - database di regole/anomalie
    - rule-based: db delle regole
    - anomaly-based: conoscenza rappresentata e aggiornata con tecniche di machine learning
  - detection engine
    - rule-based: ricerca efficiente nel db delle regole
    - anomaly-based: tecniche di machine learning

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

NIDS: problemi

presentano le difficoltà tipiche del rilevamento automatico dei problemi

- falsi positivi e negativi
- tuning difficile
- rule-based vs. anomaly-based
- difficili da comparare

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

un NIDS molto famoso

snort

- http://www.snort.org/
- rule-based
  - regole pubbliche aggiornate regolarmente
- open source
- supportato sia sotto Windows che sotto Linux

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

NIDS e reti switched

- il nids deve ispezionare il traffico (sniffer)
- sniffare reti switched è complesso
- supporto offerto dallo switch: mirroring verso una «destination port»
  - port mirroring
  - multi-port mirroring
  - vlan mirroring
- caveat
  - la banda della destination port può essere insufficiente anche se lo switch è full speed

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

NIDS: azioni

- può generare un log delle attività sospette
- può riconfigurare automaticamente un firewall
  - attività di contrasto automatica
  - detti anche intrusion prevention systems (IPS)
  - un NIDS–IPS è tipicamente in configurazione in-line con firewall incorporato
    - in sostanza un firewall con due interfacce che analizza il traffico da cui è attraversato
  - ATTENZIONE: azioni automatiche di contrasto possono attivarsi inaspettatamente e creare problemi

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

NIDS e connessioni tcp

- un NIDS non si può limitare a verificare ciascun pacchetto ip
  - cioè deve essere stateful!
- gran parte degli attacchi sono a livello applicativo e incapsulati in tcp
- è necessario seguire la sessione tcp e applicare le regole allo stream di bytes risultante
  - riordino dei segmenti tcp (e dei frammenti ipv4)
  - molto oneroso! richiede allocazione di buffer per ciascuna connessione

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

NIDS: scalabilità

- un NIDS dovrebbe essere in grado di elaborare tutto il traffico della rete
  - ogni pacchetto un lookup nel db
    - db in memoria
  - **perdita di pacchetti → perdita di accuratezza**
    - **falsi negativi**
  - le risorse necessarie dipendono da
    - numero di pacchetti
    - quantità di flussi tcp
    - quantità di segmenti fuori sequenza e uso della frammentazione

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

NIDS: load balancing

- è possibile fare cluster di NIDS con bilanciamento di carico
- **flusso**: pacchetti con la stessa quadrupla <saddr, sport, daddr, dport>
  - altra definizione di flusso possibile: stessa coppia <saddr, daddr>
- è necessario che ciascuna connessione venga analizzata dallo stesso NIDS
  - **una connessione è fatta di due flussi**
- i pacchetti di un flusso devono essere ispezionati dallo stesso NIDS nel cluster

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

switches e link aggregation (LAg)

- gli switch permettono di aggregare più link in un solo link logico (LAg)
  - utile per utilizzare due link paralleli senza spanning tree
  - autoconfigurato con il Link Aggregation Control Protocol, ieee 802.3ad
- bilanciamento del traffico sui vari link
  - ciscun flusso sullo stesso link
    - fondamentale per non desequenziare i pacchetti di un flusso – tcp inefficiente al risequenziamento massivo
  - tecnica dell'hash: link=hash(src,dst)

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

NIDS load balancing = ½ LAg

- il LAg è spesso configurabile anche staticamente
  - noi lo useremo con un solo switch!
- dietro a ciascuna porta del lag un NIDS
- mirroring di VLAN su un lag
- i lag mandano flussi identici su porte identiche e quindi sugli stessi NIDS.

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

HIDS vs. NIDS

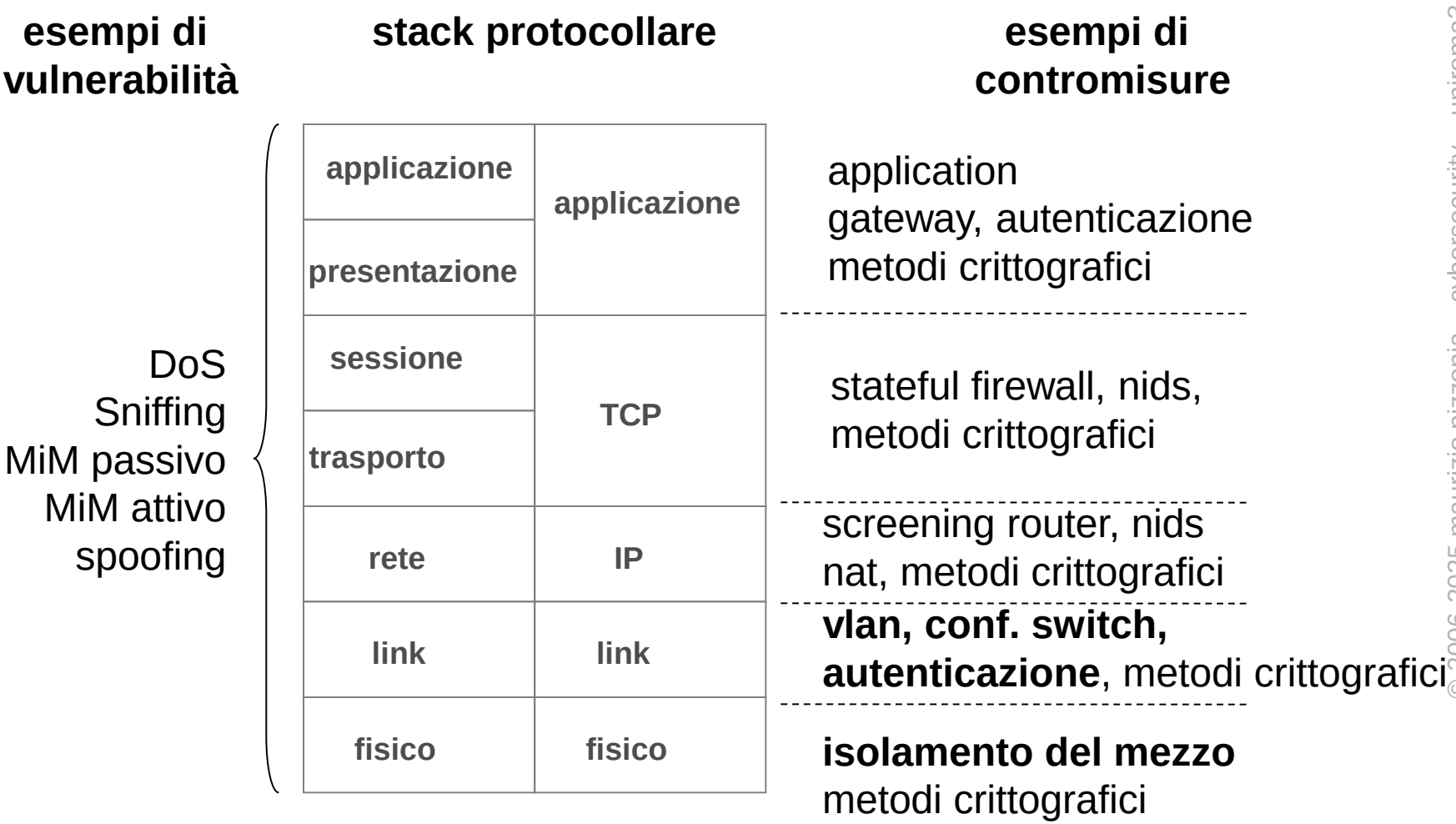
- controllano aspetti diversi
  - NIDS:
    - legittimità del traffico nella rete
  - host IDS (HIDS)
    - legittimtà del comportamento del software (integrità del sistema)
    - legittimità del traffico di rete da/per un host specifico
- approcci complementari
  - vedi prinicipio «defence in depth»

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

sicurezza delle reti
livelli 1-2

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

la sicurezza nelle reti



© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

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 con metodi quantistici: un sistema quantistico è sempre disturbato da un osservatore

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

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)

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

livello data link

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

switch

- vulnerabilità
  - mac address spoofing/flooding, broadcast storm
    - 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
  - Broadcast limit

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3

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

© 2006-2025 maurizio pizzonia – cybersecurity – uniroma3