Sicurezza nelle reti

Fondamenti di comunicazione

Schematizzazione

- Attività di comunicazione:
  - Analogica / Digitale
  - Continua / Discreta
  - Uso del mezzo (accesso)
  - Controllo di errore
  - Controllo di sequenza
  - Controllo di flusso
  - Indirizzamento in rete

Pila ISO/OSI

- 7 livelli
- Modellazione concettuale sui compiti
- A-posteriori dopo esperienza TCP/IP
- Didatticamente utile
- Va rimappata sulle esperienze:
  - TCP/IP
  - Frame relay

Livelli pila ISO/OSI

- 1 – Fisico (descrive il mezzo)
- 2 – Logico (accesso/collegamento)
- 3 – Rete (collegamento tra nodi che non si vedono)
- 4 – Trasporto (sequenza/controllo)
- 5 – Sessione (instaurazione/termine)
- 6 – Presentazione (tipi di dato)
- 7 – Applicativo (programmi)

Livello 1 - Fisico

- Cablaggio
  - Thin & Thick coax, UTP & STP, Fiber
- Connessioni
  - BNC, N, AUI, RJ45
- Modulazione
  - Baseband, telefoniche, wireless (S.S.)
- Half/Full Duplex

Livello 2 - Logico

- Sottolivello inferiore – MAC
  - CSMA, CSMA/CD, CSMA/CA
  - Token passing
  - IEEE802.3, 802.5
- Sottolivello superiore – LLC
  - Controllo errori
  - Controllo di flusso
  - HDLC, SDLC, LAPB, SLIP, PPP
- Riferimento classico: Ethernet

Livello 3 - Rete

- Invio in rete da una stazione ad un altra non necessariamente contigua
- Indirizzamento ed instradamento
- Non vi è connessione
- Non vi è controllo di consegna
- Non vi è controllo di correttezza
- Riferimento classico: IP

Livello 4 - Trasporto

- Consegna di messaggi
- Controlli di sequenza
- Controllo di flusso
- Riferimento classico: TCP
- Altro riferimento: UDP
- Endpoint
- Trasporto affidabile / inaffidabile

Livello 5 - Sessione

- Permette di iniziare / terminare una sessione
- Permette di negoziere parametri di una sessione (TWA/TWS)
- Riferimento: RAS o PPP/SLIP
- Interessante la fase di autenticazione con protocolli PAP/CHAP

Livello 6 - Presentazione

- Permette di adattare differenti presentazioni degli stassi dati (es ASCII vs EBCDIC)
- Permette di identificare differenti tipi di dati (testi/immagini/audio/video)
- Riferimento: MIME

Livello 7 - Applicativo

- E' usato dai programmi applicativi che necessitano di scambiare dati in rete:
- Riferimenti: Telnet, FTP, HTTP, SMTP

TCP/IP

- Livello 1 e 2:
  - Potrebbe essere usato così com'è ma normalmente si appoggia su:
    - Ethernet per le reti locali
    - Slip/PPP/RAS per i collegamenti ad ISP
    - FrameRelay, ATM per i collegamenti a carrier
- Livello 3: IP
- Livello 4: TCP e UDP

Imbustamento

- Normalmente nelle reti locali IP imbustato dentro Ethernet
- Necessità di costruire tabelle di collegamento tra indirizzo IP (indirizzo logico) e MAC address Ethernet (indirizzo fisico) usando ARP
- TCP o UDP imbustati in IP

Unicast, Broadcast, Multicast

- Unicast: una comunicazione diretta ad un unico indirizzo (sono le normali comunicazioni)
- Broadcast: una comunicazione diretta a tutta la rete (servono a segnalare richieste a destinatari non noti)
- Multicast: una comunicazione diretta a più indirizzi (permettono di fare economie di scala nell' invio di un messaggio a destinatari multipli)

Indirizzi

- Indirizzo fisico: esempio MAC address ethernet
  - Scritto come xx:yy:zz:ww:kk
  - Assegnato alla singola scheda dal costruttore a cui è dato da un autority
  - Individua un ***host***
- Indirizzo logico: esempio IP address
  - Scritto come aaa.bbb.ccc.ddd
  - Individua una ***rete*** ed un ***host***

Indirizzi IP: rete

- Reti di varie classi
  - 127 reti di classe A da 1 a 127 con 16.777.214 host l'una
  - 16.384 reti di classe B da 128.0 a 191.255 con 65534 host l'una
  - 2.097.152 reti di classe C da 192.0.0 a 223.255.255 con 254 host l'una
  - Indirizzi di multicast 224.x.x.x (vedere routes in Windows)

Indirizzi IP: CIDR e privati

- Classless Inter -Domain Routing
  - x.y.w.z/k
- Indirizzi privati
  - 10.0.0.0 (classe a)
  - 172.16.0.0 (classe b)
  - 192.168.0.0 (classe b)

Indirizzi IP: hosts

- Indirizzo che identifica la rete: 0
  - In realtà indirizzo con tutti i bit degli host posti a zero
- Indirizzo di broadcast: 255
  - In realtà indirizzo con tutti i bit degli host posti a uno
- Anche il MAC address di Ethernet può essere usato come broadcast ponendo tutti i bit a uno

Maschera di rete

- Identifica la parte di rete: esempio
  - 213.198.150.104 rete (/29 bit)
  - 255.255.255.248 maschera
  - 213.198.150.111 broadcast
  - Nella maschera di rete i bit relativi agli host sono a zero (gli ultimi 3)
  - Rete = Ip and mask
  - Broadcast = Rete or (not mask)

Intestazione IP

- Version, 4 bits, IPv4 = 4
- Header length, 4 bits, 4 = 20 bytes
- TOS (Type of Service), 8 bits, unused
- Packet length, 16 bits, (0-65535)
- Identifier for fragment reassembly, 16 bits
- Flags (3 bits)
  - 1 = more fragments follow, 0 = last/only fragment
- Fragmentation offset, 13 bits (0-8191)
- TTL, Time To Live, 8 bits (255-0)
  - decrement each hop, discard if 0

Intestazione IP

- Upper layer protocol, 8 bits
  - 6 = TCP, 17 = UDP, 44 = GRE
- Header checksum, 16 bits
- Source IP address, 32 bits
- Destination IP address, 32 bits
- Options (if any), 0-10 32-bit words
- Data, 0-65515 bytes

Address Resolution Protocol

- Se ci sono comunicazioni IP su ethernet l'host che inizia deve scoprire il MAC address del destinatario:
  - Invia un broadcast Ethernet con la richiesta
  - Tutti gli host ascoltano (è un broadcast)
  - Quello che ha l'IP voluto risponde
- Tabella di abbinamenti gestibile con il comando arp

Routing

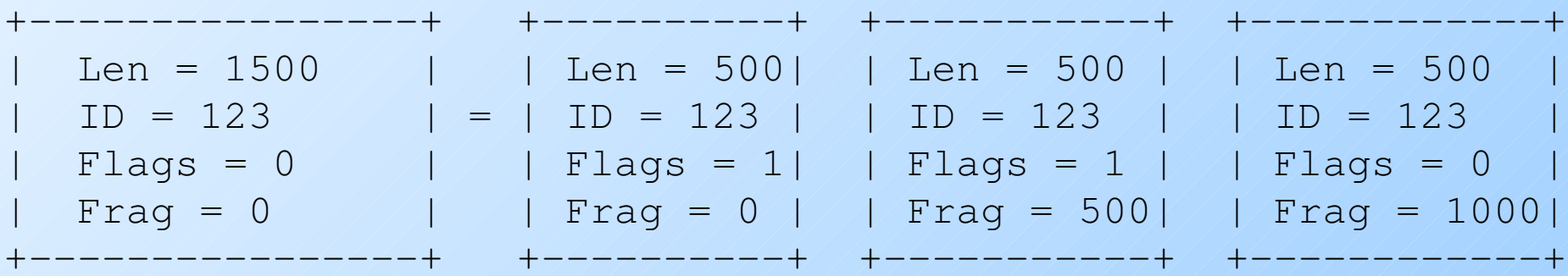
- Se si ha un default router ed il pacchetto è indirizzato fuori dalla rete
  - Viene usato ARP per trovare il MAC address del default router
  - Il pacchetto viene inviato al corretto destinatario IP
  - Il pacchetto viene inviato in un pacchetto Ethernet verso il MAC address del default router.

Frammentazione

- IP frammenta, se serve, le TPDU
  - Intestazione rimane
  - Viene seguita dalla parte del pacchetto
  - Possibile fonte di attacco
  - Nei firewall i pacchetti vanno deframmentati prima di sottoporli ad analisi

Esempio di frammentazione

- MTU = Maximum Transfer Unit
- Ethernet: MTU = 1500
- Wide area networks: MTU = 576



TCP

- TCP è il protocollo che si occupa di trasporto.
  - Protocollo affidabile (permette il riscontro delle informazioni)
  - Protocollo connesso (esiste una fase di connessione ed una di disconnessione)
  - Definisce degli endpoint (numeri di porta) a cui sono abbinabili servizi e programmi

HEADER TCP

- Source port, 16 bits (0-65535)
- Destination port, 16 bits (0-65535)
- Sequence number, 32 bits, number of bytes sent
- Acknowledgment number, 32 bits, number of bytes received
- Header length, 8 bits = 40(20+20IP) unless options are used
- Flags, 8 bits
- Receiver window size, 16 bits
- Checksum, 16 bits (XOR of header only)
- Urgent pointer, 16 bits, unused
- Options, variable length (usually 0)
- Data, variable length (usually 0-1500)

HEADER TCP FLAGS

- Unused, 2 bits
- URG, 1 bit, unused
- ACK, 1 bit,
  - 1 = received sequence through acknowledgment number
- PSH, 1 bit, unused
- RST, 1 bit
- SYN, 1 bit
  - 1 = opening connection
- FIN, 1 bit
  - 1 = closing connection

Connessione

- L'host che inizia invia un pacchetto con il flag SYN settato
- L'host che risponde invia un pacchetto con i flag SYN ed ACK settati
- Il primo host invia un pacchetto con il flag ACK settato
- La comunicazione è stabilita

Disconnessione

- L'host che intende chiudere invia un pacchetto con settato il flag FIN
- L'host che riceve un FIN risponde con due pacchetti: uno con settato l'ACK ed un altro con settato il FIN
- Il primo host risponde al FIN con un pacchetto con settato l'ACK e la comunicazione è chiusa
- C'è un tempo di attesa finale

Stato della connessione

Action	Client state	Server state
	CLOSED	LISTEN
SYN --->	SYN_SENT	SYN_RCVD
<--- SYN+ACK	ESTABLISHED	ESTABLISHED
	...	...
FIN --->	FIN_WAIT_1	CLOSE_WAIT
<--- ACK	FIN_WAIT_2	
<--- FIN	TIME_WAIT	LAST_ACK
ACK --->		CLOSED
Wait x seconds	CLOSED	

Flusso dei dati in TCP

- Sender sends packet, waits for ACK
- If checksum fails, packet is discarded
- Receiver replies with ACK, seq. number
- Sender marks data as sent
- If ACK times out, sender retransmits all unmarked data
- If same packet is ACKed 3 times, sender resends next packet (fast resend)
- Receiver ACKs all packets, including duplicates

Controllo di flusso

- Protocol to ensure that the sender does not send data faster than the receiver can receive it.
  - Receiver sends window size in ACK
  - If window is small, sender waits
  - If window size is 0, sender sends 1 byte (to get updated window in ACK)

Controllo congestione

- Protocol to ensure that the sender does not send data faster than the network can transmit it.
- Tahoe
  - Send 1 pack, wait for ACK (slow start)
  - Send 2, 4, 8, … up to threshold, wait for ACK
  - If timeout, divide threshold by 2 and go back to 1, 2, 4, 8…
- Reno (most commonly used)
  - Fast retransmission after 3 ACKs
  - Fast recovery, cancel slow start after 3 ACKs
- Vegas
  - Uses round trip delays to predict congestion

HEADER UDP

- Source port, 16 bits (0-65535)
- Destination port, 16 bits (0-65535)
- Length in bytes, 16 bits (0-65535)
- Checksum, XOR of header, 16 bits

USO UDP

- Flussi di dati non connessi
  - DNS (vedi oltre)
  - Allineamento data/ora
- Necessità di velocità
  - Trasferimenti audio/video
- RemoteProcedureCall
  - Base per NFS ed altri
  - Spostano affidabilità al livello 7
  - Fonte di pericoli (1 porta più servizi)

ICMP

- Internet Control Message Protocol
- Messo nella parte dati di IP

Tipo	Codice	
8	0	Echo request by ping
0	0	Echo reply to ping
11	0	TTL expired (usato da traceroute)

ICMP

Tipo	Codice	
3	0	Destination network unreachable
3	1	Destination host unreachable
3	2	Destination protocol unreachable
3	3	Destination port unreachable
3	6	Destination network unknown
3	7	Destination host unknown
4	0	Source quench (unused, congestion control in TCP)
9	0	Router advertisement (used by RIP)
10	0	Router discovery
12	0	IP header bad

IPV4/IPV6

- IPV4 – Versione attuale
- IPV6 – Nuova versione
  - Indirizzi IP più lunghi (128 bit)
  - Nessun checksum
    - si usa quello del TCP o del data link layer
  - Nessuna frammentazione
    - I pacchetti troppo lunghi sono scartati
  - Non ci sono le opzioni
    - Si usano quelle del protocollo imbustato

IPV6

- Version, 4 bits, IPv6 = 6
- Priority, 4 bits, replaces TOS
- Flow, 24 bits, identifier for special data types
- Payload length, 16 bits (0-65535)
- Next header, 8 bits (TCP or UDP)
- Hop limit, 8 bits (same as TTL)
- Source address, 128 bits
- Destination address, 128 bits
- Data (cannot exceed MTU)

DNS

- Protocollo per risolvere i nomi
- Utilizza UDP
- Utilizza la porta 53
  - Uno dei pochi casi in cui si deve aprire una porta UDP sui firewall
- Allineamento tra NS
  - Utilizza TCP
  - Utilizza la porta 53

SNMP

- Permette di gestire apparecchiature di rete che lo supportano (switch, routers, stampanti)
- Permette di leggere e scrivere proprietà
- Permette di ricevere segnalazioni
- Basato su UDP
- 'Sicuro' solo su rete locale, la versione 1 ha seri problemi di sicurezza

SMTP

- Simple Mail Transfer Protocol
- Protocollo applicativo basato su TCP/IP
- Opera generalmente sulla porta 25
- Usato per scambiare mail
- Facilmente contraffacibile
  - Indirizzo IP mittente
  - Unico dato 'vero' normalmente è l'indirizzo IP di provenienza

Fasi SMTP (1)

- Helo
  - Helo **dominio**
  - Inizia una fase di spedizione
  - Molti mailer verificano il dominio
  - Problemi con modifiche Verisign
- Mail from
  - Mail from: **utente@dominio**
  - Indica il mittente
  - Si può, al massimo, controllare il dominio

Fasi SMTP (2)

- Rcpt to
  - Rcpt to: **utente**
  - Indica il destinatario
- Data
  - Inizia la trasmissione dei dati
  - In formato RFC822
  - Terminati con .
- Quit
  - Termina la connessione

Fasi SMTP (3)

- Dati
  - Headers
    - Mail from
    - Subject
    - Date
    - ...
  - Linea vuota
  - Contenuti
  - Tutti i dati sono contraffacibili

POP3

- Postal Office Protocol
- Utilizza TCP/IP su porta 110
- Uso in Internet va verificato
  - Utente tramite ISP lo usa in rete locale
  - Utente tramite ISP è autenticato da user/passwd alla connessione
  - Usare imbuti crittografici, VPN o versione crittografata (pop3s porta 995)

Sessione POP3 (1)

- User
  - User **utente**
  - Pass **password**
- List
  - Ottiene la lista dei messaggi
- Retr
  - Retr **msg#**
  - Ottiene il messaggio

Sessione POP3 (2)

- Dele
  - Dele **msg#**
  - Cancella il messaggio
- Quit
  - Termina il lavoro

IMAP

- Internet Mail Access Protocol
- Lavora usando TCP/IP sulla porta 143
- Più potente di POP3
  - Permette la gestione della posta sul server di posta sul quale può organizzarla per folder
- Stesse problematiche di sicurezza di POP3, ma con maggiori rischi

Sessione IMAP (1)

- Login
  - **sessid** login **user passwd**
    - a001 login peppe pappa
- Select inbox
  - **sessid** select inbox
    - A001 select imbox
  - Ottiene lo stato della casella con la posta in ingresso

Sessione IMAP (3)

- Logout
  - **sessid** logout
    - a001 logout
  - Termina il collegamento
- Molti altri comandi: quelli visti bastano a testare il protocollo

HTTP

- Hyper Text Transfer Protocol
- Serve a scaricare pagine web
- Usa protocollo TCP/IP porta 80
  - Attenzione: in http si può indicare una qualsialsi porta
- Esiste HTTPS che usa la crittografia ed opera normalmente sulla porta 443

Sessione HTTP

- Reperisce la pagina desiderata
  - GET **url**
    - GET http://www.mgeng.com
  - Formato 0.9 accettato in tutte le versioni del protocollo

FTP

- File Transfer Protocol
- Usa due sessioni: controllo e dati
- La sessione di trasferimento dati viene aperta dal server e non dal client
  - C'è un comando (passive) per far aprire la sessione dati dal client in modo da poter uscire da firewall
- Sessione controllo usa TCP porta 21
  - Sessione dati di default userebbe porta 20

Comandi FTP (1)

- user
  - user **user**
  - passwd **password**
- cd **directory**
  - Cambia directory sul server
- lcd **directory**
  - Cambia directory sul clent

Comandi FTP (2)

- pwd **directory**
  - Scrive la directory usata sul server
- dir oppure ls
  - Lista il contenuto della drectory
- get **file**
  - Trasferisce il file dal server al client
- put **file**
  - Trasferisce il file dal client al server

Comandi FTP (3)

- hash
  - Fa apparire un segno # ogni tot bytes trasferiti durante un'operazione di get o put
- mget **filespec**
  - Trasferisce più file dal server al client
- mput **filespec**
  - Trasferisce più file dal client al server

Comandi FTP (4)

- prompt
  - attiva/disattiva la richiesta di conferma di trasferimento ad ogni file da parte dei comandi mget/mput
- ascii
  - Seleziona il trasferimento di tipo testuale
- bin
  - Seleziona il trasferimento di tipo binario

Comandi FTP (5)

- passive
  - attiva/disattiva il modo passivo (connessione dati iniziata dal client) usato per uscire dai firewall
- quit
  - Termina il lavoro

Strumenti

- Ifconfig/ipconfig: verifica schede
- Route: verifica indirizzamento
- Arp: verifica tabelle ARP
- Ping: verifica collegabilità
- Traceroute: verifica percorso
- Nslookup: verifica nomi
- Tcpdump: visualizza dati

- Ifconfig/ipconfig

- Serve a vedere i dati delle interfacce di un pc
  - Indirizzi IP
  - Maschera di rete
  - Statistiche
- Utilizzabile per configurare un interfaccia

Route

- Route print su piattaforma Win
- Route su piattaforma Linux
  - Eventualmente route -n per vedere solo i numeri senza la risoluzione dei nomi
  - Route add, route del per modificare la tabella di routing
  - Usabile anche sui server
  - Esiste un comando più versatile (ip)

ARP

- Il comando arp permette di vedere l'arptable
- Utile per ricavare i mac-address delle schede di rete se si vogliono usare per le policy sui firewall oppure sui DHCP
- Si può utilizzare per introdurre o cancellare dei valori nella tabella che viene normalmente riempita dal protocollo ARP

PING

- Usa il protocollo ICMP per chiedere un echo ad un server e misurare l'IRTT
- Può essere usato per inserire nell'arp table un mac address
- Può essere usato per forzare una risoluzione del nome
- Può essere usato per stressare la rete (ping -f)

Traceroute

- Basato su ICMP
- Gioca con Time to live in modo da far generare dei messaggi ICMP (11/0) di TTL spirato in modo da conoscere il server inviante
- Molti firewall filtrano ICMP
- Molti router non trasmettono più segnalazioni ICMP (11/0)

Nslookup

- Permette la verifica dei nomi
- Uso semplice: nslookup server per ottenre l'indirizzo IP del server
- Uso interattivo più complesso ma più potente.
  - Si lancia il comando nslookup
  - Si usano i vari comandi

Comandi Nslookup

- server nome
  - Permette di impostare un differente server DNS a cui inviare le query
- set type=**tipo**
  - any significa qualunque informazione
  - mx significa gli indirizzi dei mailer
  - ptr significa risoluzione inversa (cerca il nome dato l'indirizzo)

tcpdump

- Permette di tracciare i pacchetti che passano nella rete
- Limitato dall'utilizzo degli switch che inviano il traffico solo all'host interessato
- Utile come strumento di analisi dei pacchetti e del funzionamento dei firewall