

[Applications]

- Client/Server Model
- Ftp
- Dns
- Telnet
- Rsh/Rexec
- NFS
- Sntp, POP, Imap
- Http
- SNMP
- LPR, LDP

[Security]

- Common Attacks
 - Tapping the wire
 - Impersonation
 - Denial-Of-service
 - Replay of Messages
 - Guessing of Passwords
 - Guessing of keys
 - Viruses

[Security (cont)]

- Solutions
 - Encryption
 - Authentication by digital signatures and certificates
 - Authorization
 - Integrity checking and message Authentication codes
 - Non-repudiation
 - One-time passwords and two-way random number handshakes
 - Frequent key refresh, strong keys and prevention of deriving future keys
 - Address concealment

[Security Implementation]

- Ip filtering
- NAT
- IPSec
- SOCKS
- SSH
- SSL
- Application Proxies
- Firewalls
- Kerberos and Authentication Servers
- Secure Electronic Transactions

[Firewalls]

- Can be standalone device, a router or even PC
- Splits up more secure networks from less secure networks
- Packet-Filtering Router
- Application-Level Gateway (proxy)
- Circuit Level Gateway

[Packet Filtering Router]

- Extract information from header
 - Source IP
 - Destination IP
 - TCP/UDP Source Port
 - TCP/UDP destination Port
 - ICMP message type
 - Encapsulated protocol information (TCP, UDP, ICMP or IP tunnel)
- Service Level Filtering
- Source/Destination Level Filtering
- Packet Filtering is quite complicated in cases of exceptions and leaves holes

[Gateways]

- Application Level Gateway
 - Proxy acts as a server to the client and as a client to the destination
 - Proxy seems transparent
 - Gives application level filtering
 - Client has to change especially on authentication
 - Can act as a gateway to private IP network
- Circuit Level Gateway
 - Transparent Gateway
 - Pass all information once user is authenticated

[Network Address Translation]

- Assumes small number of hosts are communicating outside of the private network
- Will map an internal address to a public one
- When a mapping is done, checksum needs to be calculated again
- Needs to know when address can be returned to pool, this is normally a timeout of 15 mins
 - Can use Fin packets for TCP connections
- Mapping may also be static
- When applications share IP addresses, Nat will fail (ex ftp)
- When using IPSec, NAT fails since integrity is not maintained