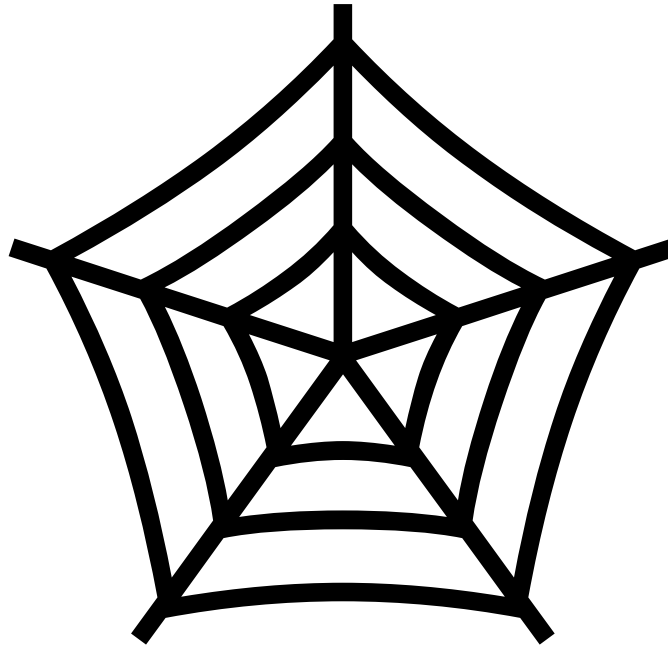
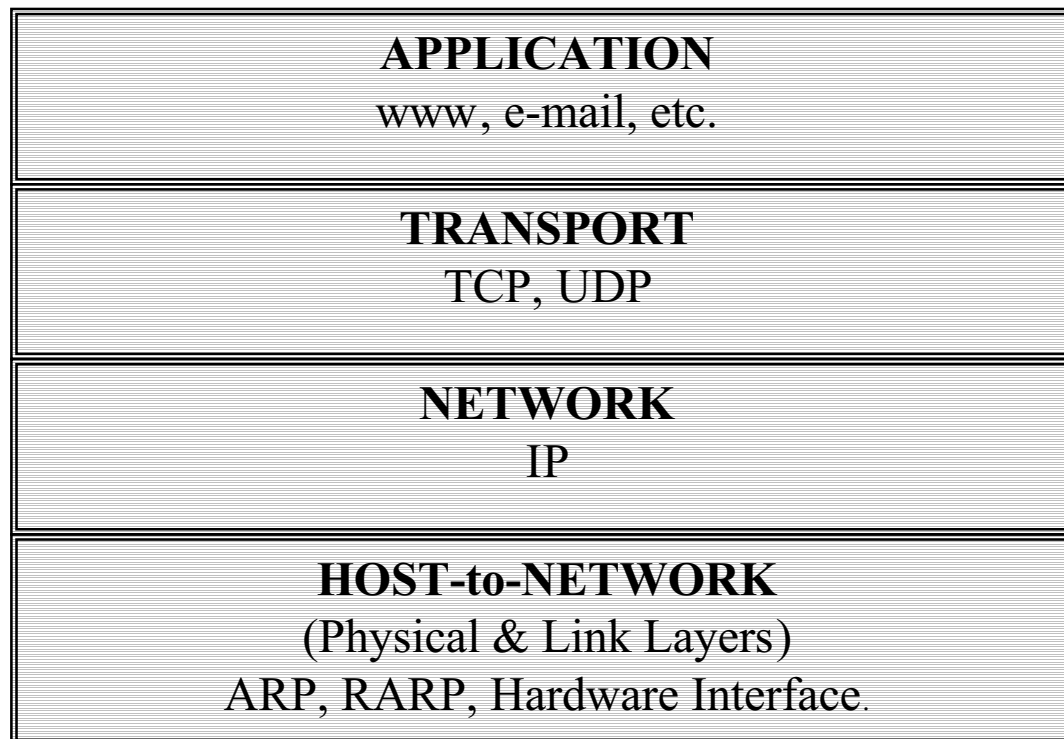

Internet Protocol Security Flaws



TCP/IP Protocol Suite

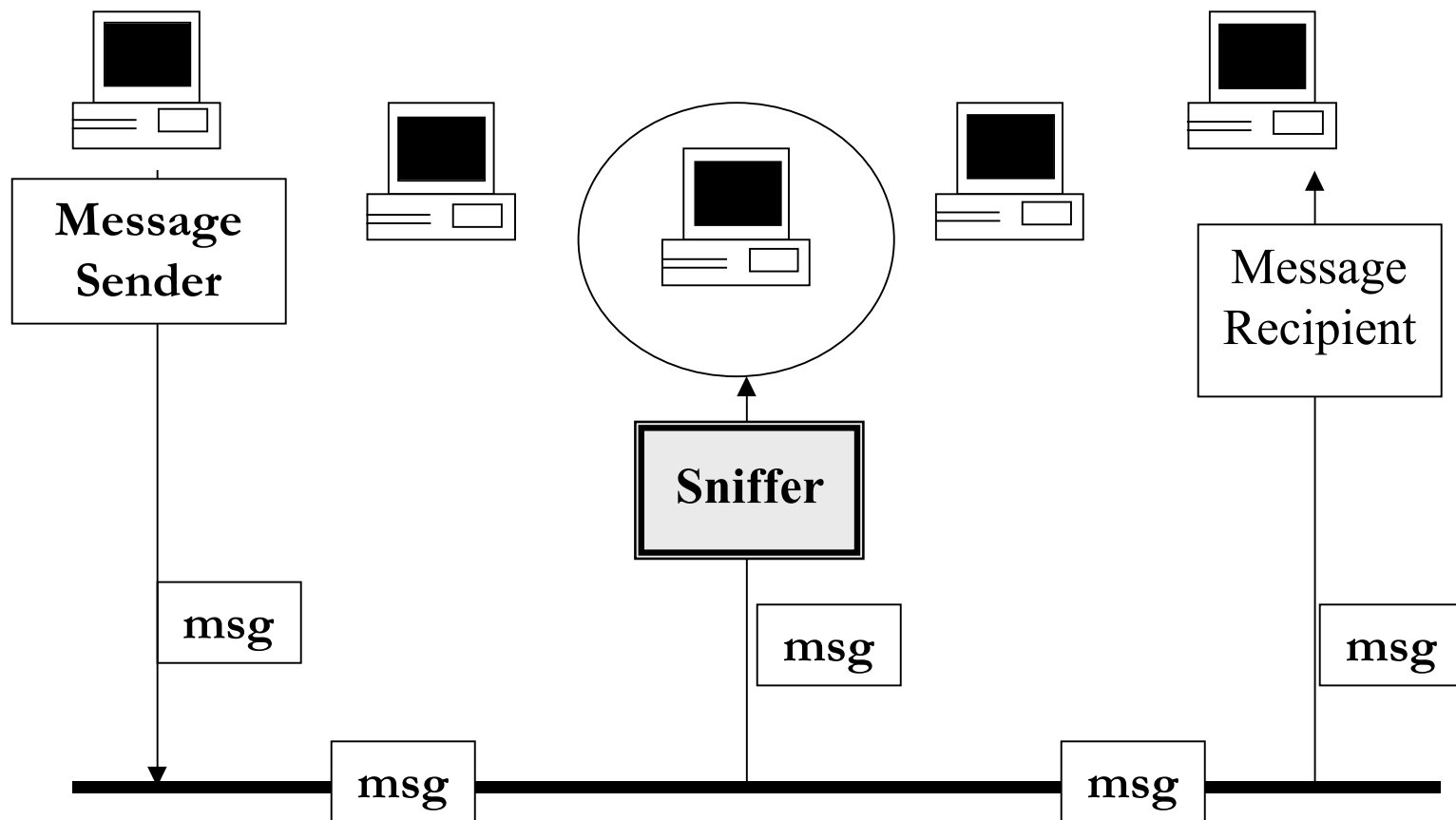


Security at the IP Layer

- Network Sniffing
- Message Replay
- Message Alteration
- Message Delay and Denial



Sniffing an Internet Message

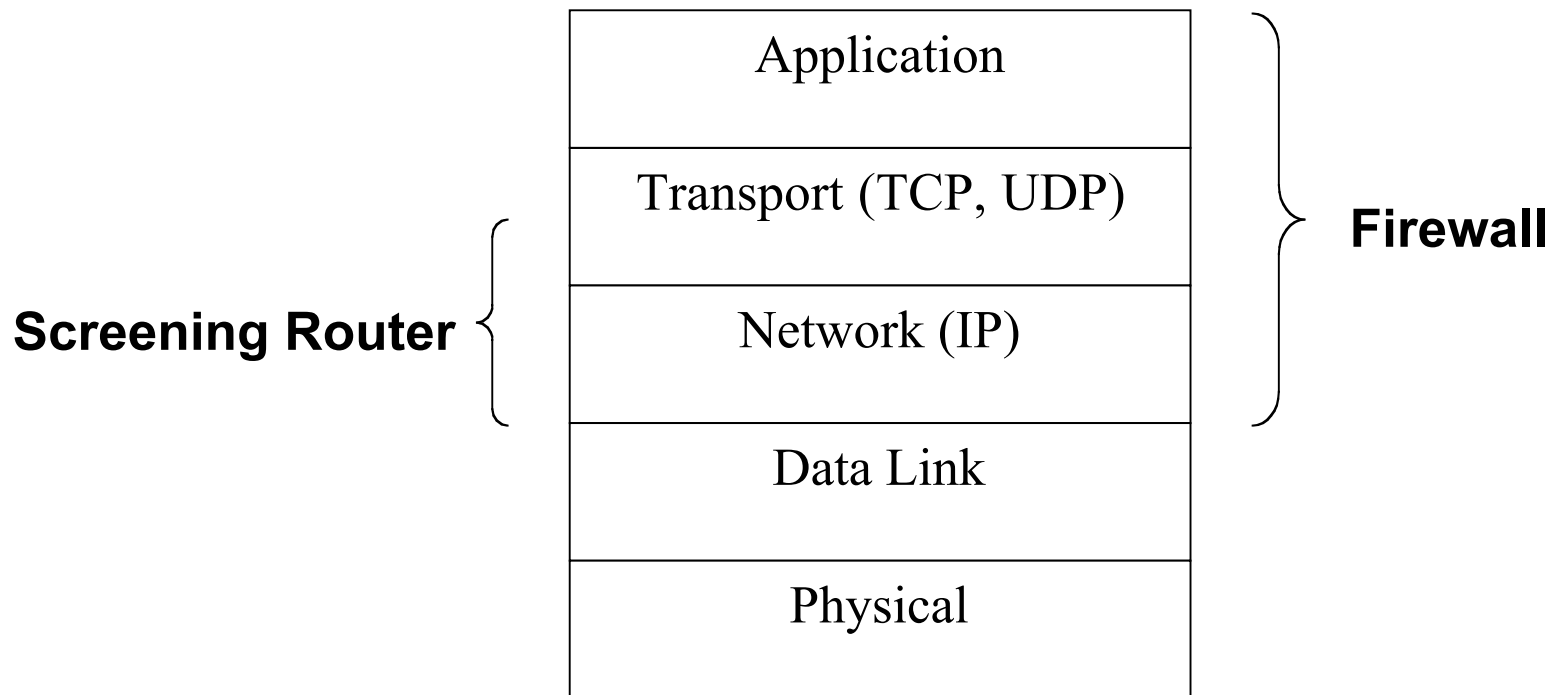


Authentication Issues at the IP Layer

- Address Masquerading
- Address Sniffing



Unauthorised Access





MSc in Information Security
Royal Holloway

Routing Attacks

ROUTING ATTACKS

Security at the Transport Layer

- Similar security risks and problems as with the IP Layer
- Packet Filtering
- Hijacking



Internet Worm

- Not a virus - Worm can be run by itself
- Disrupted over 6,000 computers using security loops in applications closely associated with OS.
- Basic object to get shell on another machine so it can further reproduce. Three ways it attacks



Sendmail Attack

Worm opens TCP connection to another machine's sendmail, invokes debug mode, requests data be piped through a shell

Fingerd Attack

Tries to infiltrate system using bug in fingerd.

Rsh/Rexec Attack

Went through /etc/passwd file trying to guess passwords.



Denial of Service Attacks

“No one should deliberately attempt to degrade or disrupt system performance or to interfere with the work of others.”

Mail bombing

Ping flooding

"Smurf attacks"

"SYN flooding"



PPTP Security Flaws

- Point to Point Tunneling Protocol (PPTP)
- PPTP enables implementation of secure, multi-protocol Virtual Private Networks (VPN's), through the Internet.
- VPN - enables remote locations to appear to be local. This is done without the expense incurred from running leased lines or dedicated cabling to each location, and is sometimes called a “tunnel”.



PPTP Security Flaws

- The concept of PPTP is becoming increasingly popular with companies.
- However, companies using Microsoft products to implement their Virtual Private Networks may find that their Networks are not so private



Bruce Schneier - Counterpane Systems

- Counterpane Systems: a cryptography and computer security consulting firm.
- Bruce Schneier (assisted by expert hacker; Peter Mudge) carried out a Cryptanalysis of Microsoft's PPTP.
- As a result, many security flaws were found in Microsoft's **implementation** of PPTP.
- **Note:** No flaws were actually found in the PPTP protocol itself.



Major Flaws

- Password Hashing: weak algorithms allow eavesdroppers to learn the user's password. Also, use of common passwords allow dictionary attacks to occur.
- Challenge/Handshake Authentication Protocol: a design flaw allows an attacker to masquerade as the server.



Major Flaws

- Encryption: implementation mistakes allow encrypted data to be recovered.
- Encryption Key: security of the key is no greater than the security of the password.
- Control Channel: unauthenticated messages let attackers crash PPTP servers.



Additional Attacks

A host of additional attacks were also identified;

- Bit Flipping - an attacker can undetectably flip bits in the ciphertext, without any knowledge of the encryption key or the client's password.
- Passive Monitoring - by setting up a standard sniffer, MS PPTP servers can be easily monitored.
- Spoofing Point-to-Point Negotiations.
- Packet Resynchronization.



Conclusion for MS PPTP Flaws

- In a market study by Infonetics Research, PPTP was found to be the most popular VPN protocol currently in use.
- This is probably because it's
 - a) Free in a Microsoft environment &
 - b) generally applicable.
- Microsoft promises to fix the problem as soon as possible
But Schneier feels that the quick fix may be worse than the problem!



Conclusion for MS PPTP Flaws

The product manager for Windows NT Security, states the following in a weak attempt to put the flaws in perspective;

➤ *“The CIA spends billions of dollars on security, but our customers do not need that level of security!”*





MSc in Information Security
Royal Holloway

Secure Socket Layer

SSL Handshake Protocol

SSL Record Protocol



Strength of the SSL Protocol

- Dictionary Attack
- Brute Force Attack Against Strong Ciphers
- Replay Attack
- Man-In-The-Middle Attack



Omission from the SSL Specification

- Certification Management
- Error Messages



Weaknesses of the SSL Protocol

- Brute Force Attack Against Weak Ciphers
- Renegotiation of Session Keys
- Other weaknesses



Historical Faults Found in SSL

- Netscape Random Numbers
- PKCS #1



Secure- HTTP

- Designed to secure HTTP connections
- Provides confidentiality, authentication & integrity
- General nature of S-HTTP makes difficult to assess exactly what threats are, but similar to those against SSL.
- Problem ensuring keys transferred properly.
- Programmer not familiar with cryptography might think S-HTTP would protect him and totally fail to provide any cryptographic protection



SSH (Secure Shell)

- SSH- Secure Shell and is a secure login program.
- Very powerful application using strong cryptography to protect all transmitted confidential information
- Security flaw if attacker has access to encrypted SSH stream. He may insert encrypted blocks in stream that will decrypt to arbitrary commands to be executed on SSH server.



More SSH

- Very difficult attack to perform. Requires extensive knowledge of TCP/IP network & SSH protocol
- Security flaw of protocol.





MSc in Information Security
Royal Holloway

No More :)

The End

