

Foundations of TCP/IP Security

Anton J Aylward
System Integrity
AJA@SI.on.ca
(416) 421-8182

Foundations of TCP/IP

Security

Objectives

- **Learn**
 - Basic Concepts
 - Key Terms
 - Security Issues
- **Avoid Bafflement**

Foundations of TCP/IP Security

- Fundamentals and Background
- Vulnerabilities
- About Firewalls

Foundations of TCP/IP

Security

- Confidentiality
- Integrity
- Availability
- Authentication
- Auditability

Foundations of TCP/IP Security

- **Fundamentals and Background**
- Vulnerabilities
- About Firewalls

Fundamentals

- Terminology
- History
- Lessons Learnt

Terminology

ISO - International Standards Organisation

IETF - Internet Engineering Task Force

TCP - Transmission Control Protocol

IP - Internet Connection

UDP - User Datagram Protocol

ICMP - Internet Control Message Protocol

Terminology - ISO Reference Model

7	APPLICATION
6	PRESENTATION
5	SESSION
4	TRANSPORT
3	NETWORK
2	DATA LINK
1	PHYSICAL

Terminology - ISO Reference Model

- Application Layer (7)
 - Services required by User Interfaces
 - Deals with “meaning” of data
 - Only communicates with layer 6

Terminology - ISO Reference Model

- Presentation Layer (6)
 - Data Representation
 - Syntax not “meaning”
 - Only communicates with layers 7 and 5

Terminology - ISO Reference Model

- Session Layer (5)
 - Synchronisation
 - Ordering of data flow
 - Only communicates with layers 7 and 5

Terminology - ISO Reference Model

- Transport layer (4)
 - Provides reliable transparent data transfer
 - Hides details of technology
 - Order Exchange
 - Only communicates with layers 5 and 3

Terminology - ISO Reference Model

- Network Layer (3)
 - Provides message routing & relaying
 - Independent of protocol used
 - Provides
 - Network Services
 - Flow Control
 - Load Handling
 - Only communicates with layers 4 and 2

Terminology - ISO Reference Model

- Data Link Layer (2)
 - Manages communication between adjacent system
 - Independent of Network Access Method
 - Accuracy by
 - Frame Formatting
 - Error handling
 - Addressing
 - Only communicates with layers 3 and 1

Terminology - ISO Reference Model

- Physical layer (1)
 - Electrical encoding of the transmission
 - Access to physical network
 - Only communicates with layer 2

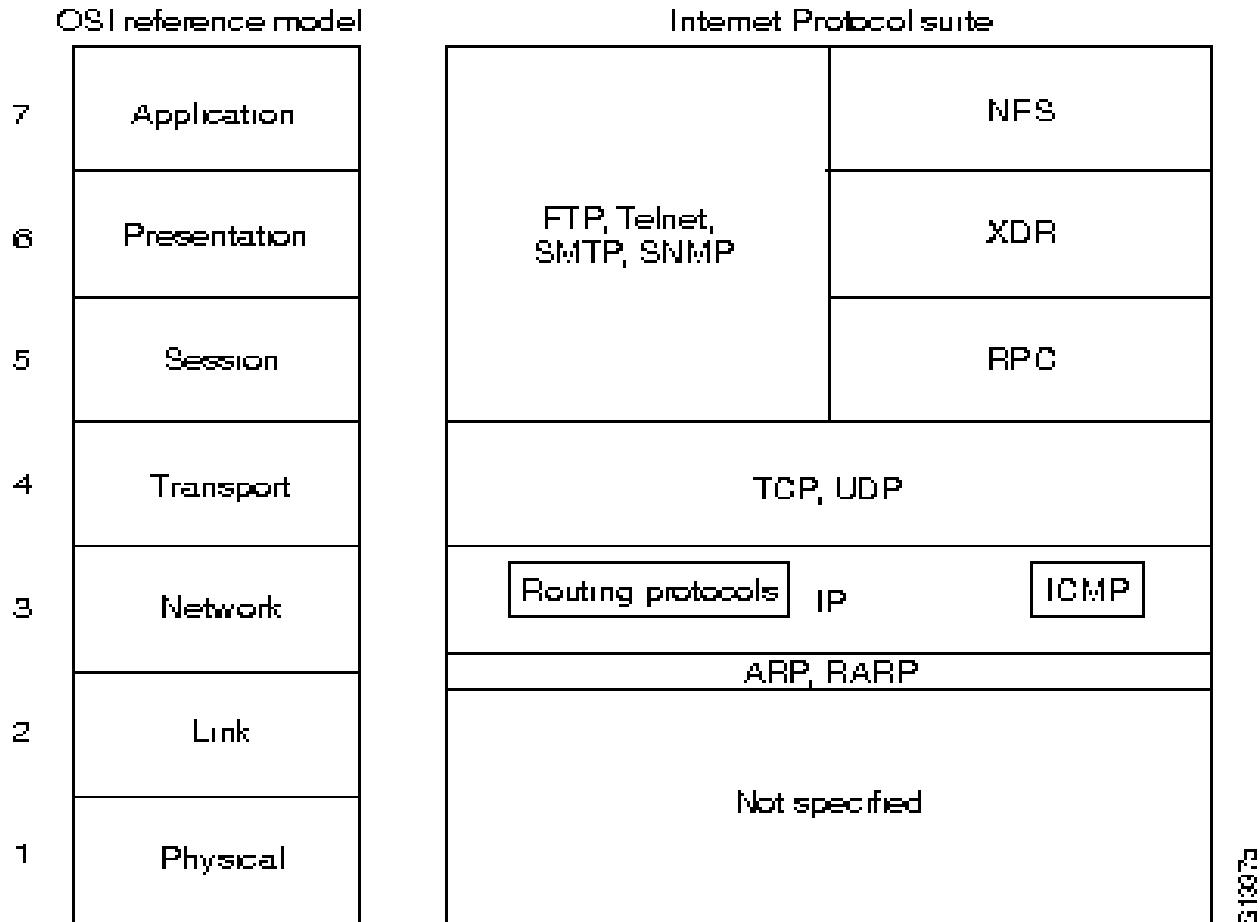
Terminology - ISO Reference Model

- Great in Theory
- Gives a Good Vocabulary
- Insight into what we already knew
- Unusable in practice

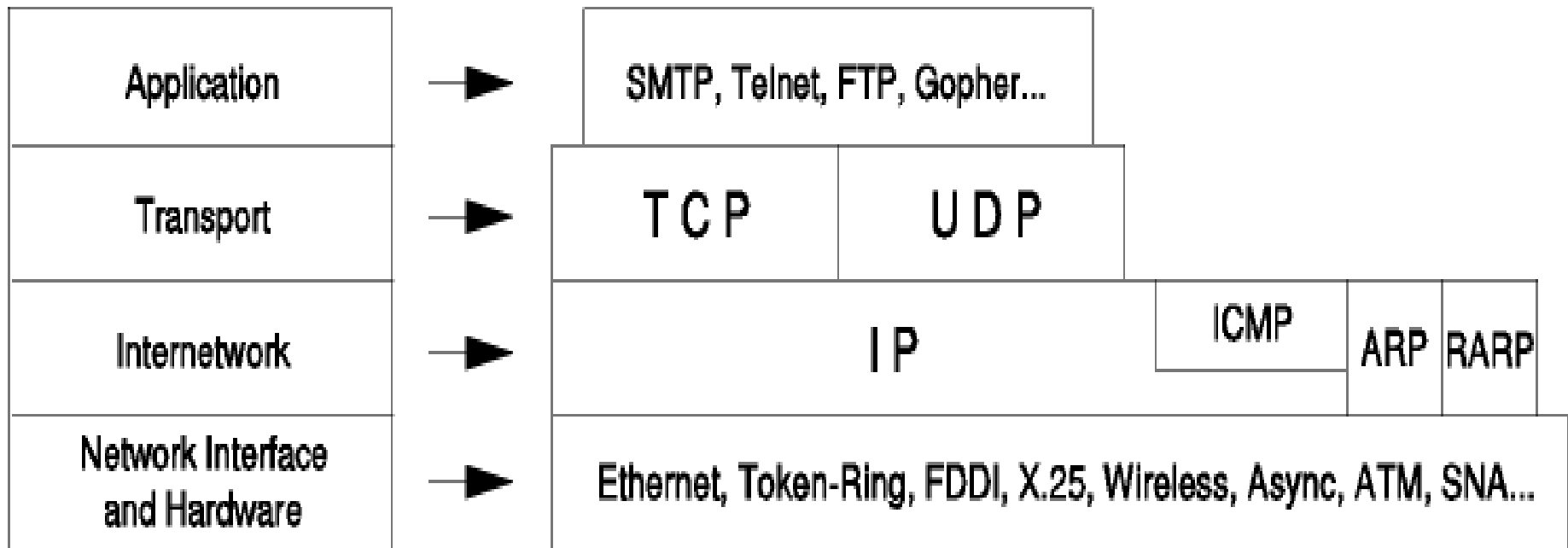
Terminology - TCP/IP Model

- A SUITE of protocols
 - Different roles for different needs
- Open Architecture
 - Define the what not the how
 - “If you have a better idea, share it freely, or make use of mine”
- Pragmatic Development
 - No Ivory Tower
 - Theory and Practice hand in hand

Terminology - TCP/IP Model



Terminology - TCP/IP Model

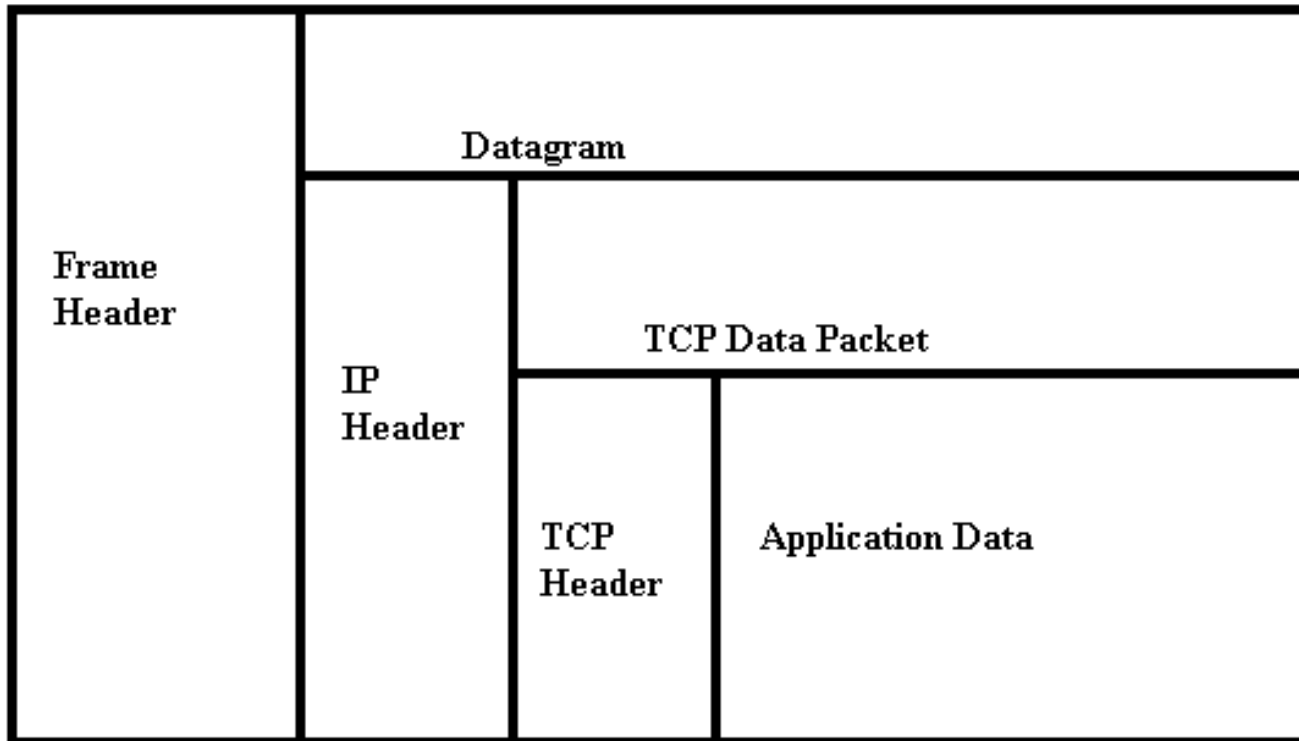


Frame Format - TCP/IP Model

Nesting of Data/Packets

- TCP is carried by
- IP is carried by
- Ethernet MAC

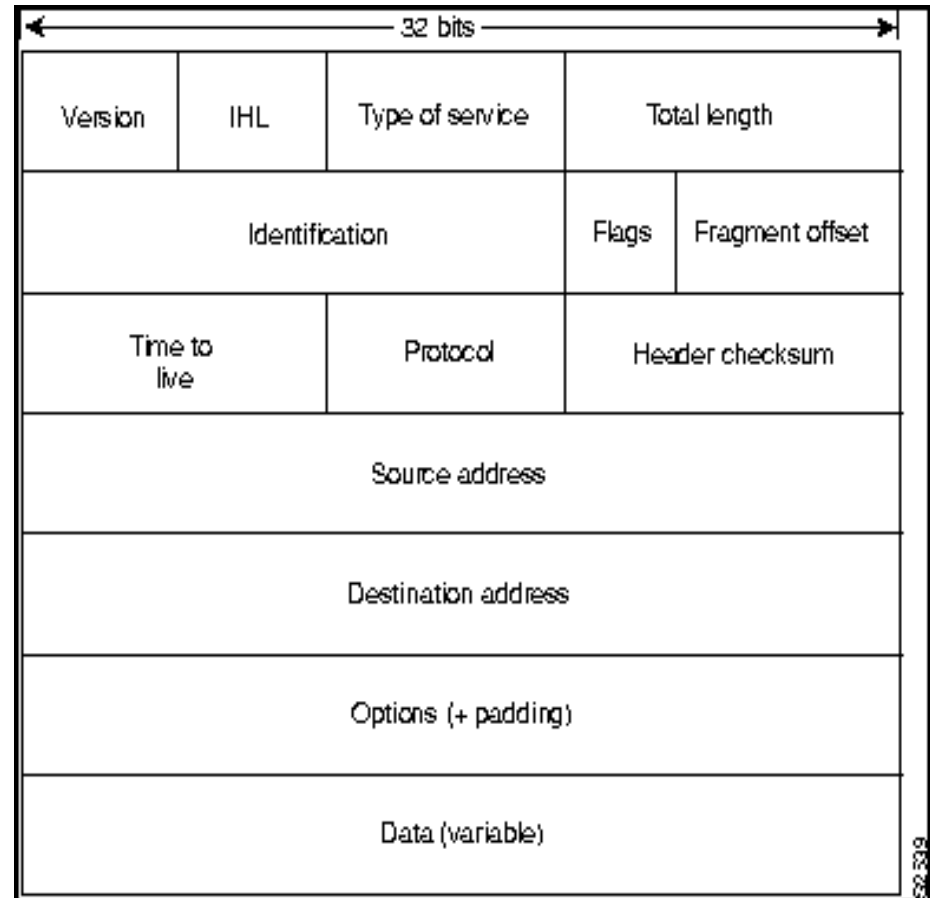
Frame Format - TCP/IP Model



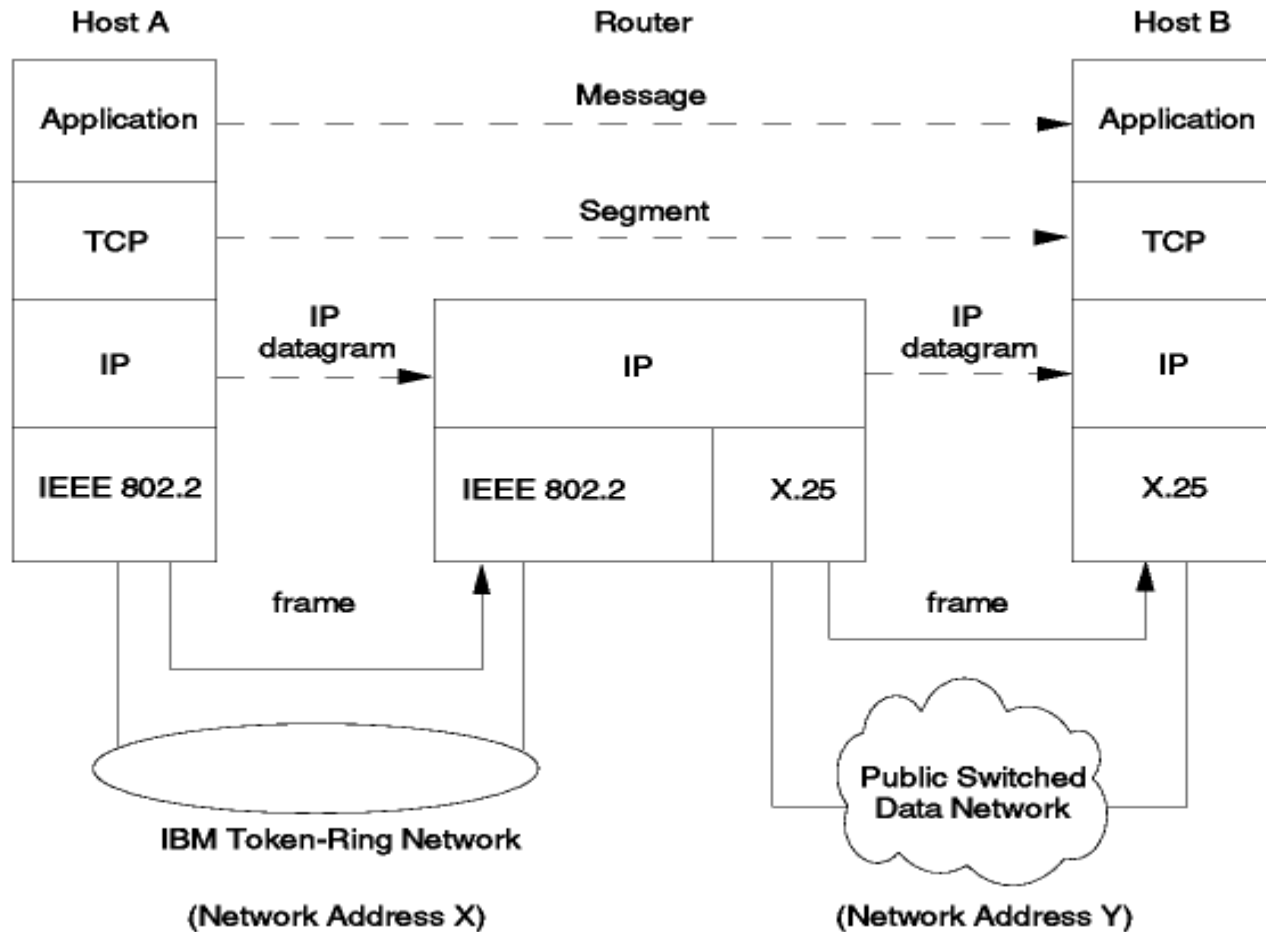
Frame Format - TCP/IP Model

TCP Header

- Source
- Destination
- Protocol
- Payload
- Option



TCP/IP Networking Model



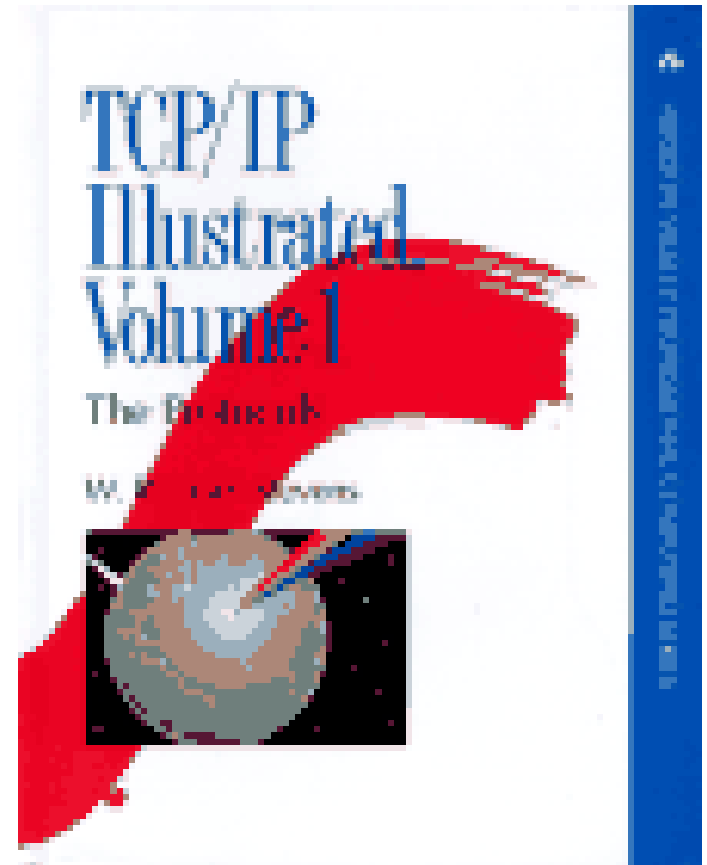
TCP/IP- Reading List

TCP/IP Illustrated

Richard Stevens

Addison-Wesley

ISBN: 0-201-63346-9



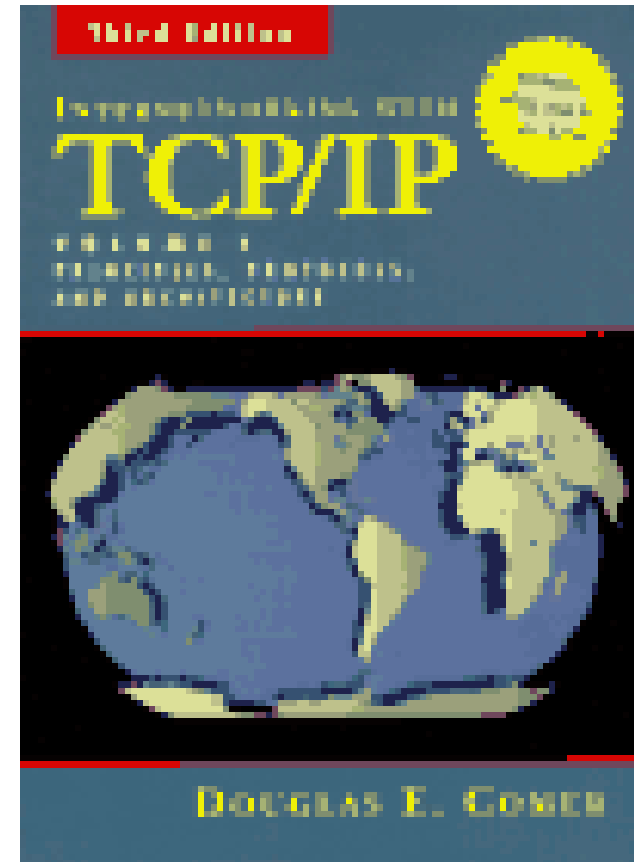
TCP/IP- Reading List

Internetworking With
TCP/IP

Doug Comer

Prentice Hall

ISBN: 0-132-16987-8



Foundations of TCP/IP

Security



Pause for Questions

Foundations of TCP/IP Security

- Fundamentals and Background
- Vulnerabilities
- About Firewalls

Vulnerabilities

Subagenda

- Protocols
- Services
- Components

Vulnerabilities - The 80/20 Rule

80% of your problems are internal

- Poor Configuration
- Inadequate Controls
- Lack of Training and Awareness
- “Finger Trouble”

Vulnerabilities

- **Hackers get all the publicity**
- **Errors and Omission cause all the problems**

Vulnerabilities - Global not TCP/IP

- audio/video viewing
- audit suppression
- backup theft, corruption, or destruction
- below-threshold attacks
- breaking key management systems
- bribes and extortion
- cable cuts
- call forwarding fakery
- cascade failures
- collaborative misuse
- combinations and sequences
- content-based attacks
- covert channels
- cryptanalysis
- data aggregation
- data diddling
- dependency analysis and exploitation
- desynchronization and time-based attacks
- device access exploitation
- distributed co-ordinated attacks
- dumpster diving
- earth movement
- electronic interference
- emergency procedure exploitation
- environment corruption
- environmental control loss
- error insertion and analysis

Vulnerabilities - Global not TCP/IP

- error-induced misoperation
- errors and omissions
- excess privilege exploitation
- false updates
- fictitious people
- fire
- flood
- get a job
- hangup hooking
- hardware-system failure-flaw exploitation
- illegal value insertion
- imperfect daemon exploits
- implied trust exploitation
- inadequate maintenance
- inadequate notice exploitation
- defaults
- induced stress failures
- infrastructure interference
- infrastructure observation
- input overflow
- insertion in transit
- interprocess communication attacks
- interrupt sequence mishandling
- invalid values on calls
- kiting
- man-in-the-middle
- modelling mismatches
- modification in transit
- multiple error inducement
- network service and protocol attacks
- observation in transit

Vulnerabilities - Global not TCP/IP

- password guessing
- PBX bugging
- peer relationship exploitation
- human engineering
- piggybacking
- power failure
- privileged program misuse
- process bypassing
- protection missetting
- exploitation
- race conditions
- reflexive control
- relocation
- repair/replace/remove information
- replay attacks
- repudiation
- residual data gathering
- resource availability manipulation
- restoration process corruption or misuse
- salami attacks
- selected plaintext
- severe weather
- shoulder surfing
- simultaneous access exploitations
- solar flares
- spoofing and masquerading
- static
- strategic or tactical deceptions

Vulnerabilities - Global not TCP/IP

- sympathetic vibration
- system maintenance
- testing
- Trojan horses
- undocumented or unknown function exploitation
- van Eck bugging
- viruses
- volcanos
- wire closet attacks



Vulnerabilities - Protocols

Is TCP/IP any more vulnerable than any other networking protocol?

NO

- Open
- Component Oriented

Vulnerabilities - Protocols

- Protocol Subversion
 - Second Most popular ‘hacker attack’
- Spoofing
 - DNS Subversion
 - Others
- Session Hijacking
 - Mitnick & Shimomura - “Takedown”

Vulnerabilities - Services

Most Common “Hacker Attack”

- Poor Configuration
 - Back Doors
 - Passwords
 - Un-needed Services
- “Stack Smashing”
 - Poor Coding
 - Few programmers code with security in mind
 - Unsuitable hardware

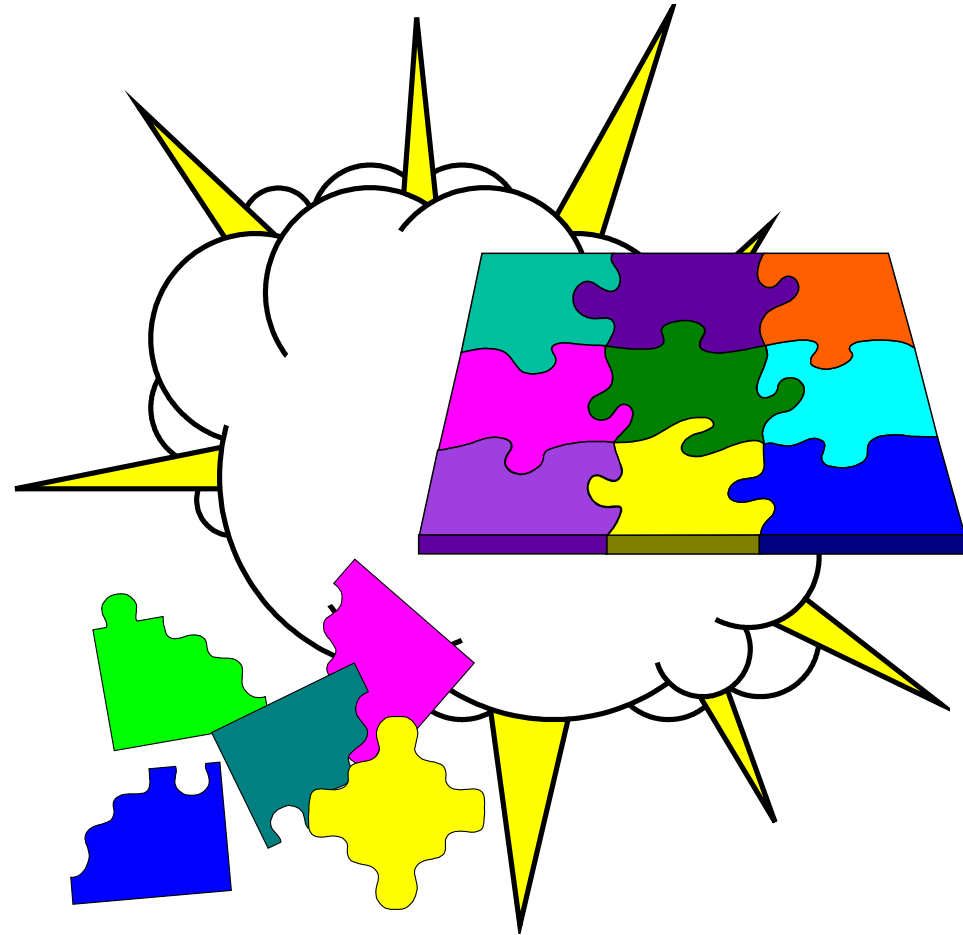
Vulnerabilities - Services

Defending Services

- Don't Run Unnecessary Services
- Do read the CERT Notices
- Apply Vendor Patches Promptly
- Get Sources !!! (GNU/LINUX)
- Check Configuration Files
- **KEEP IT SIMPLE**

Vulnerabilities -Components

- Programming Errors
- Buffer Overflow
- Library Spoofing
- Poor Discipline
- “User Friendly”
- “Quick & Dirty”
- Trojans
- Lack of Understanding



Design Examples



Pause for Questions

Foundations of TCP/IP Security

- Fundamentals and Background
- Vulnerabilities
- About Firewalls

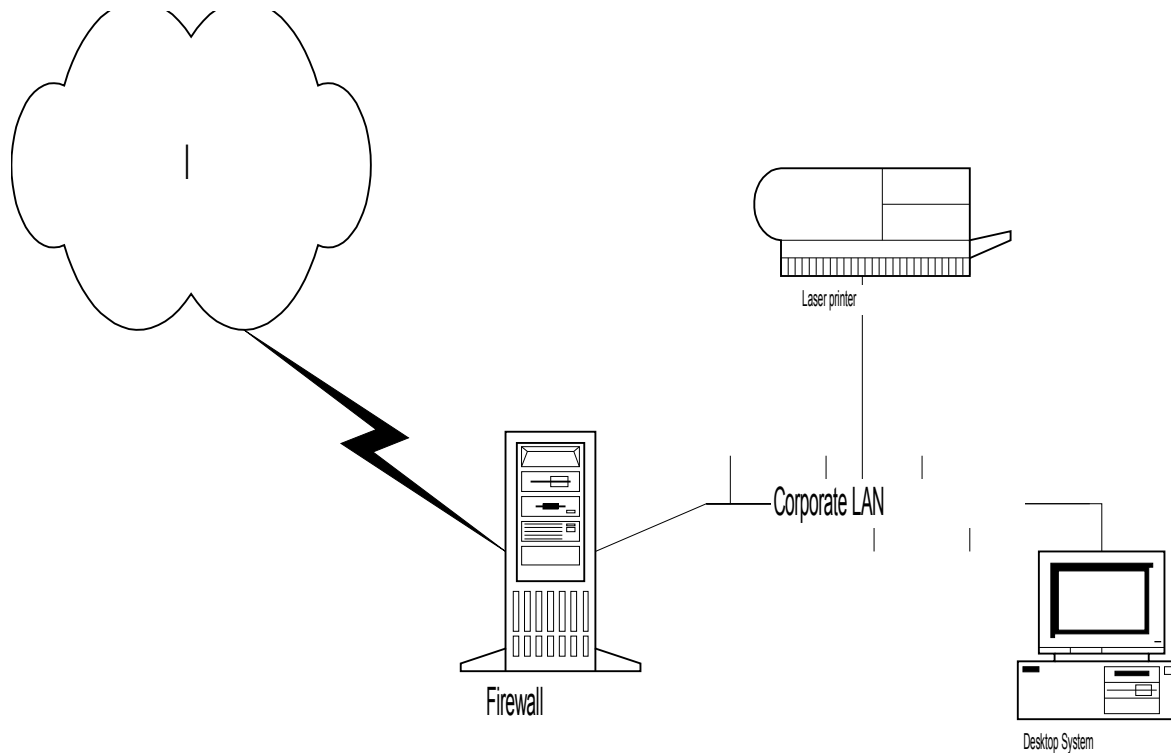
Design Examples

AGENDA

- The Myth of the Firewall
 - What it Isn't
 - Perimeter
 - Policy
- An Example Gateway
 - Firewall Components
 - Mail Handling

The Myth of The Firewall

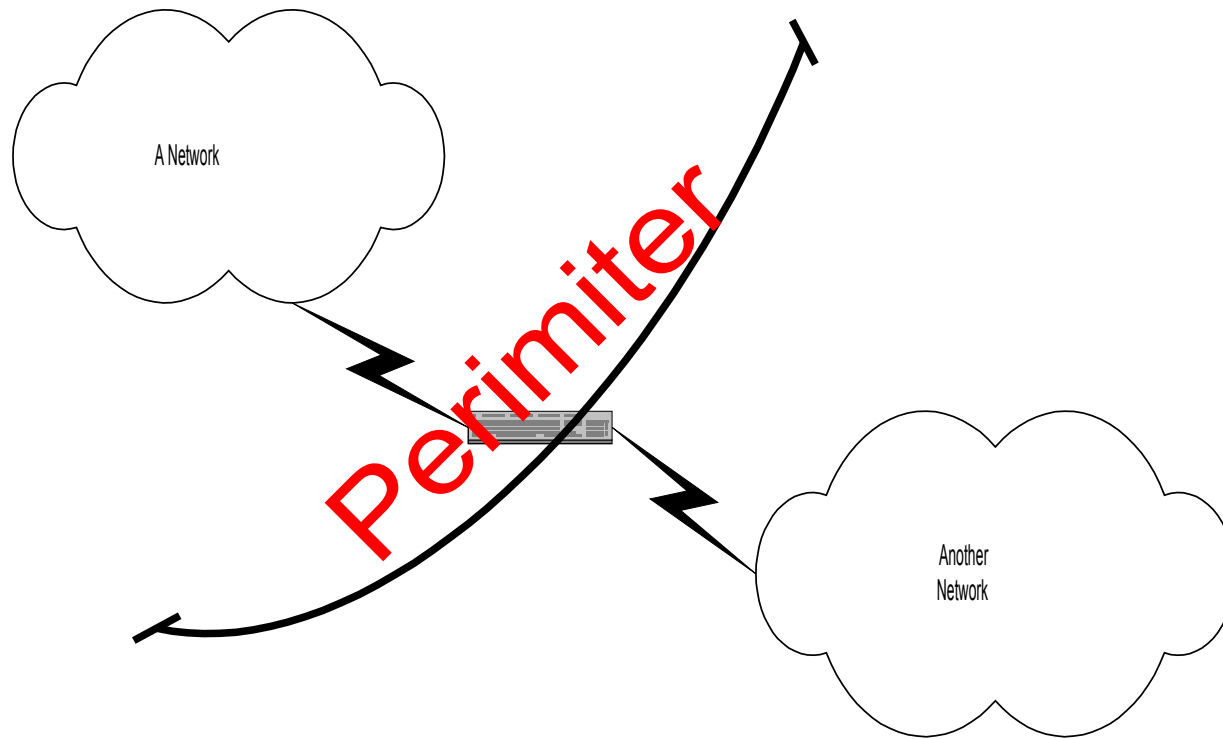
So You Think You Are Protected By The Firewall?



The Myth of The Firewall

- You can't buy it in a box ready built
 - Despite what salesmen tell you
- Its not a Firewall, its a **Perimeter Protection Policy Enforcement Mechanism**
- If you don't have Policy
- You're working blind
- If you don't define the Perimeter
- You can't defend it

The Myth of The Firewall



The Myth of The Firewall

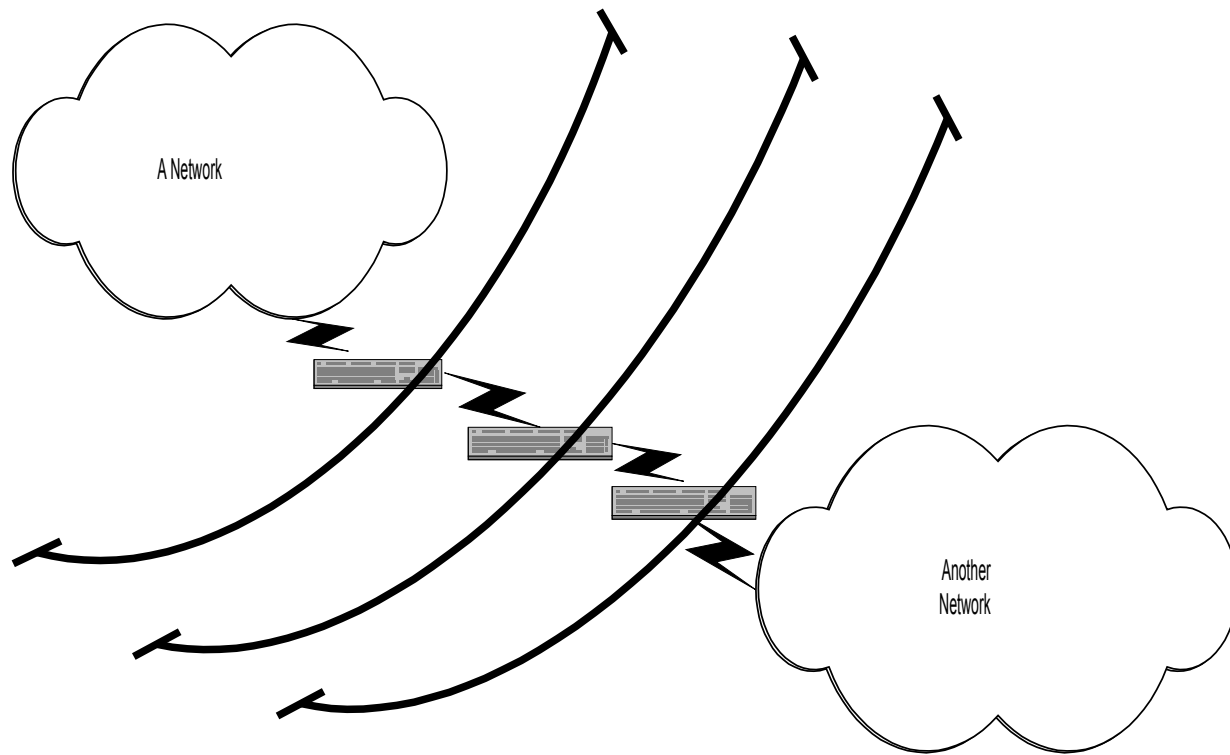
Where to Put the Firewall

- At the Single Point of Access to the Internet
- Internally?
 - Do you want the guys in R&D to access Payroll?
 - The Executive Suite
 - Different policies in different places

Firewall - Terminology

- DMZ
- Bastion Host
- Packet Filtering
- Dual Homed
- Transparency
- Logging
- Authentication
- VPN/Tunnelling
- Screened Subnet
- Screening Router
- TCP & UDP
- IP Options
- Fragmentation
- MAC & ARP
- ACK/NACK

Firewall - Defence in Depth

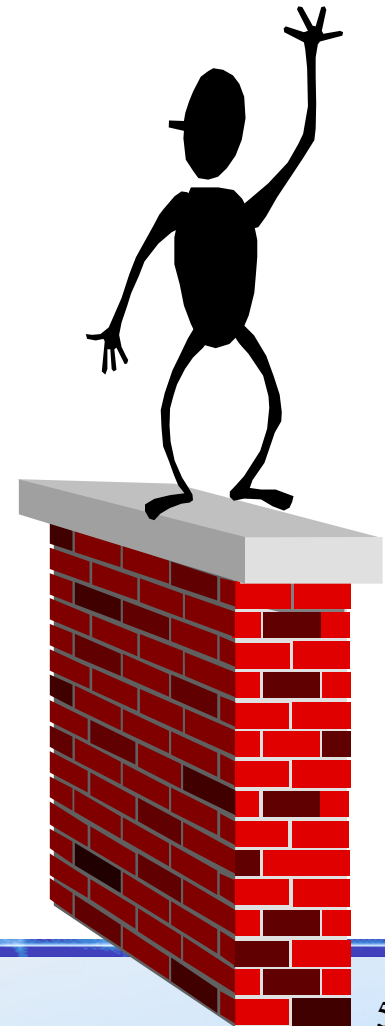


Firewall - Also does ...

- Enforces trust relationships
 - Different networks have different levels, groups
- Provides an Audit Trail
- Performs Authentication
- Minimises size of “Zone of Risk”
- Opportunity for Better Management Controls
- Addresses Legal Responsibilities

Firewall - Proxies

- “On behalf of”
- Implies higher level functions
 - “knowledge” of the application
 - making decisions based on content and context
- E-Mail - Store and Forward Proxy



Firewalls - Categories

Used to be called “gateways”

- Packet Filters
 - Implemented in Routers
 - Still a powerful tool
- Application Level
 - Pioneered by Marcus Ranum at DEC, 1992
 - Evolved into “proxies”
- Circuit Level
 - Protocol & TCP Aware

Firewall - Proxies

Debasement of Terminology

- Circuit Layer Proxy
 - Basic router filter
- Traffic Aware Proxy
 - knows about TCP but not the data
- Command Aware Proxy
 - e.g. For FTP
- Content Aware Proxy
 - Mail Virus Scanning
- Policy Aware Proxy
 - Theoretical

Firewalls - Packet Filters

- Certain Protections can only be provided by packet filtering
 - Address Spoofing
- Others Cannot
- Doesn't require user knowledge
 - Transparent
- Packet filtering *Should* be fast
- Not easy to modify
- Not Universal

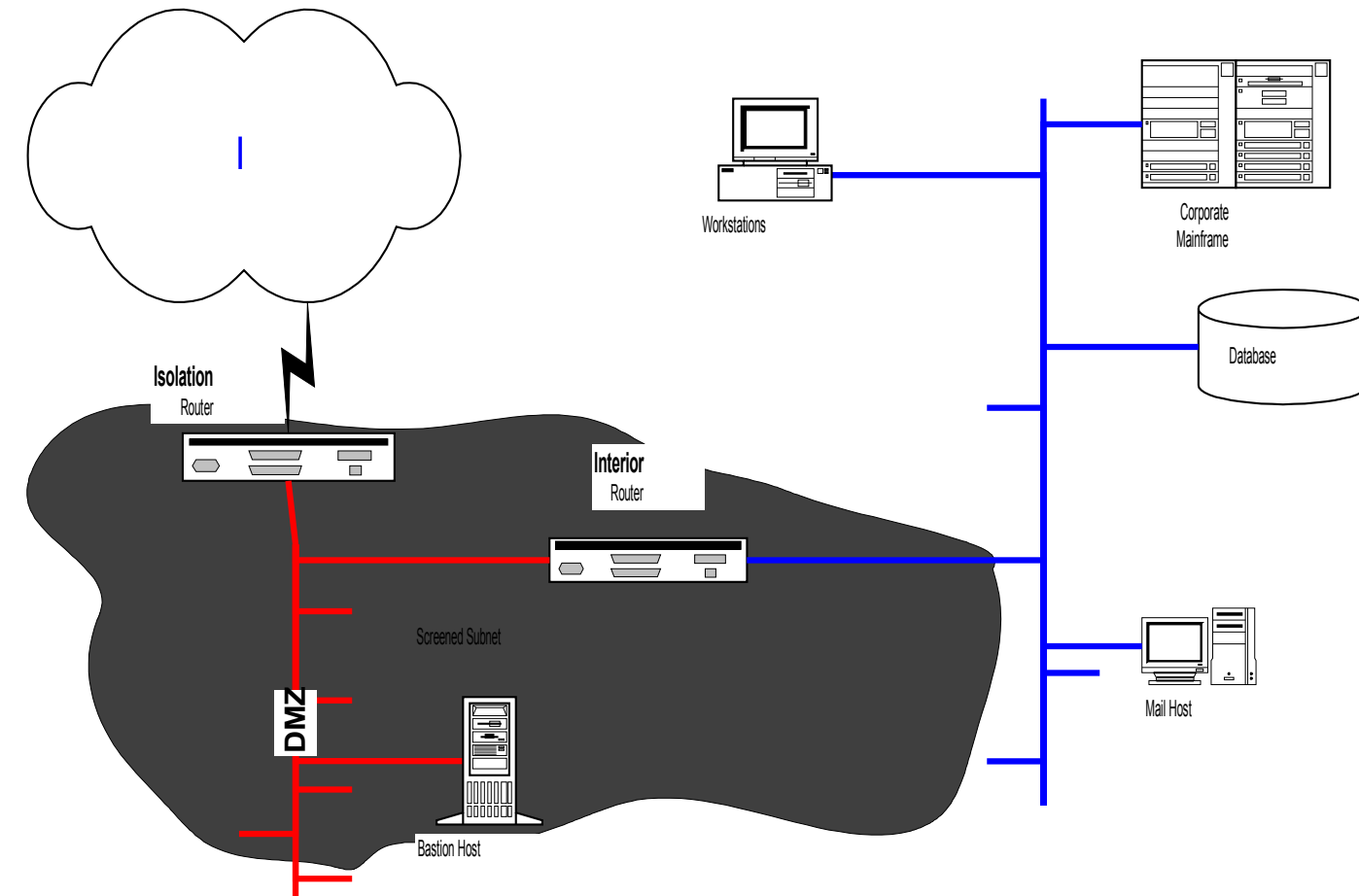
Firewalls - Circuit

- Protocols above IP
 - TCP UDP ICMP RPC
- TCP - Connection Oriented
 - Start-up handshake
 - Teardown
 - Sequence Number
- UDP - No connection
- ICMP - Status and Control
- RPC - Remote Procedure Call
 - Difficult to filter

Firewalls - Application

- Sometimes called Proxies
- Specific to Applications
- Usually “outbound”
- More Overhead
 - ... but evolving to Stateful Inspection
- Can be very intelligent, granular
 - Rule driven
- Can be transparent
- Easy to Customise

Design Example - Real System



Design Example - Real System

Security Benefits

- Isolation
- Failure Resistant
- Layered Protection
- Separation of Duties/Functions
- Least Privilege
- Manual Operations

Design Example - Real System

Isolation Router Filters

- Only permit incoming to Bastion from Internet
- Only Permit outgoing from Bastion to Internet
- Deny ALL traffic between Internet and Interior router

Design Example - Real System

Interior Router Filters

- Only permit incoming from Bastion
- Only Permit outgoing to Bastion
- Deny ALL traffic between internal network and Isolation router

Design Example - Real System

Bastion Host Host

- Runs Proxies
- Implements Policies
- Performs logging
- Translates internal names/addresses to external
- ?? VPN ??

Reading Material

- Papers by Marcus Ranum, Lots of them
 - Early papers at DEC
 - Many Papers on Firewall Principles
 - Recent papers on Intrusion Detection
- Steve Bellovin
 - Security Problems with TCP
 - Primary References on Firewall Principles
- Brent Chapman
 - Problems with Router based filters

Foundations of TCP/IP Security

Thank you for
Attending