INFS 766/INFT 865
Internet Security Protocols

Lectures 1 and 2
Firewalls and Their Limitations

Prof. Ravi Sandhu

REFERENCE BOOKS

- Network Security Essentials, William Stallings, Prentice-Hall, 2000
- Security Technologies for the World Wide Web, Rolf Oppliger, Artech House, 2000
- Internet and Intranet Security, Rolf Oppliger, Artech House, 1998
- Building Internet Firewalls, Brent Chapman and Elizabeth Zwicky, O'Reilly and Associates, 1995
- Network Security: Private Communication in a Public World, C. Kaufman, R. Perlman and M. Speciner, Prentice-Hall, 1995

2

WEB SOURCES

- source for RFCs and IETF
  - http://www.ietf.org
- cryptographic sources
  - RSA's frequently asked questions: http://www.rsa.com/rsalabs/newfaq
  - NIST encryption home page: http://csrc.nist.gov/encryption/
- firewall sources
  - Links to many vendor sites: http://www.waterw.com/~manower/vendor.html
  - Firewalls mailing lists and searchable archive: http://lists.gnac.net/firewalls
  - Firewalls frequently asked questions: http://www.clark.net/pub/mjr/pubs/fwfaq

3

SECURITY COURSES CYCLE

- **Fall**
  - **INFS 762 Information Systems Security**
  - **INFS 767 Secure Electronic Commerce**
- **Spring**
  - **INFS 766 Internet Security Protocols**
  - **INFS 765 Database Security**
  - **INFT 862 Formal Models for Computer Security**

4

OPENING REMARKS

INTERNET INSECURITY

- **Internet insecurity spreads at Internet speed**
  - **Morris worm of 1987**
  - **Password sniffing attacks in 1994**
  - **IP spoofing attacks in 1995**
  - **Denial of service attacks in 1996**
  - **Email borne viruses 1999**
- **Internet insecurity grows at super-Internet speed**
  - **security incidents are growing faster then the Internet (which has roughly doubled every year since 1988)**

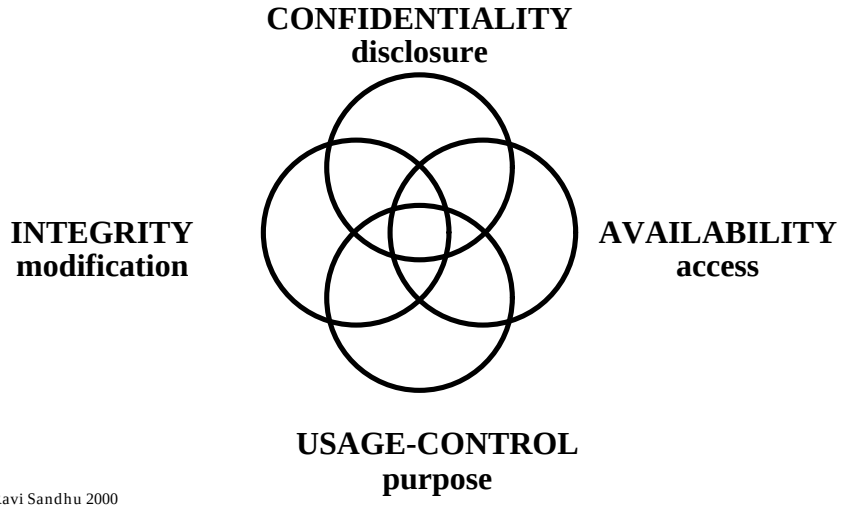
6

INTERNET SECURITY

- There are no clear cut boundaries in modern cyberspace
  - AOL-Microsoft war of 1999
  - Hotmail password bypass of 1999
  - Ticketmaster deep web links

7

SECURITY OBJECTIVES



8

SECURITY TECHNIQUES

- **Prevention**
  - **access control**
- **Detection**
  - **auditing/intrusion detection**
  - **incident handling**
- **Acceptance**
  - **practicality**

9

THREATS, VULNERABILITIES ASSETS AND RISK

- **THREATS are possible attacks**
- **VULNERABILITIES are weaknesses**
- **ASSETS are information and resources that need protection**
- **RISK requires assessment of threats, vulnerabilities and assets**

10

RISK

- **Outsider Attack**
  - **insider attack**
- **Insider Attack**
  - **outsider attack**

11

PERSPECTIVE ON SECURITY

- **No silver bullets**
- **A process NOT a turn-key product**
- **Requires a conservative stance**
- **Requires defense-in-depth**
- **A secondary objective**
- **Absolute security does not exist**
- **Security in most systems can be improved**

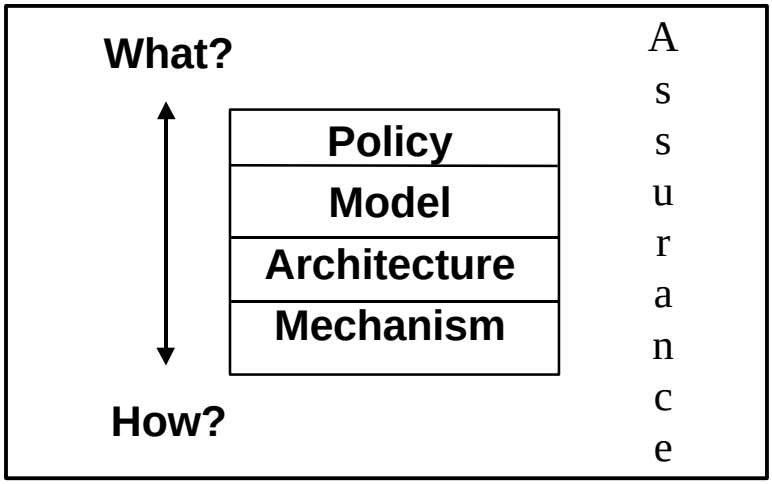
12

PERSPECTIVE ON SECURITY

- **absolute security is impossible does not mean absolute insecurity is acceptable**

13

ENGINEERING AUTHORITY & TRUST 4 LAYERS



14

INTRUSION SCENARIOS

CLASSICAL INTRUSIONS SCENARIO 1

- **Insider attack**
  - **The insider is already an authorized user**
- **Insider acquires privileged access**
  - **exploiting bugs in privileged system programs**
  - **exploiting poorly configured privileges**
- **Install backdoors/Trojan horses to facilitate subsequent acquisition of privileged access**

16

CLASSICAL INTRUSIONS SCENARIO 2

- **Outsider attack**
- **Acquire access to an authorized account**
- **Perpetrate an insider attack**

17

NETWORK INTRUSIONS SCENARIO 3

- **Outsider/Insider attack**
- **Spoof network protocols to effectively acquire access to an authorized account**

18

DENIAL OF SERVICE ATTACKS

- **Flooding network ports with attack source masking**
- **TCP/SYN flooding of internet service providers in 1996**

19

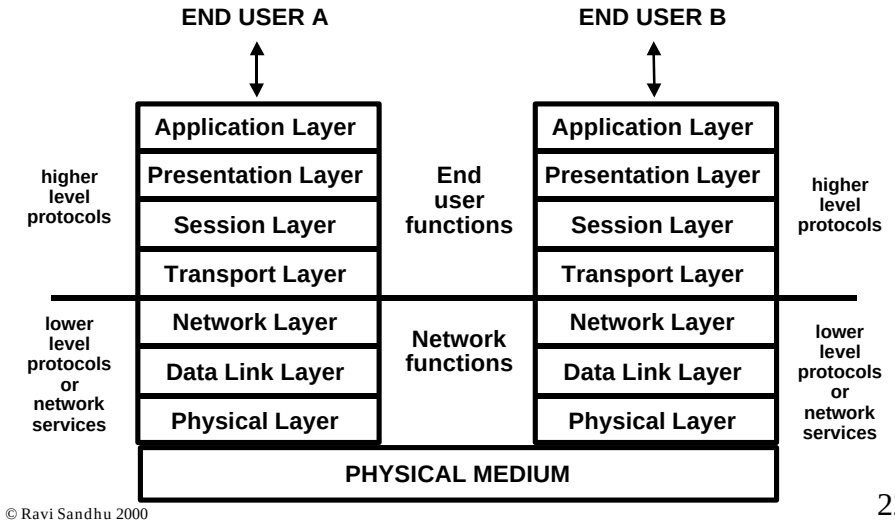
INFRASTRUCTURE ATTACKS

- **router attacks**
  - **modify router configurations**
- **domain name server attacks**
- **internet service attacks**
  - **web sites**
  - **ftp archives**

20

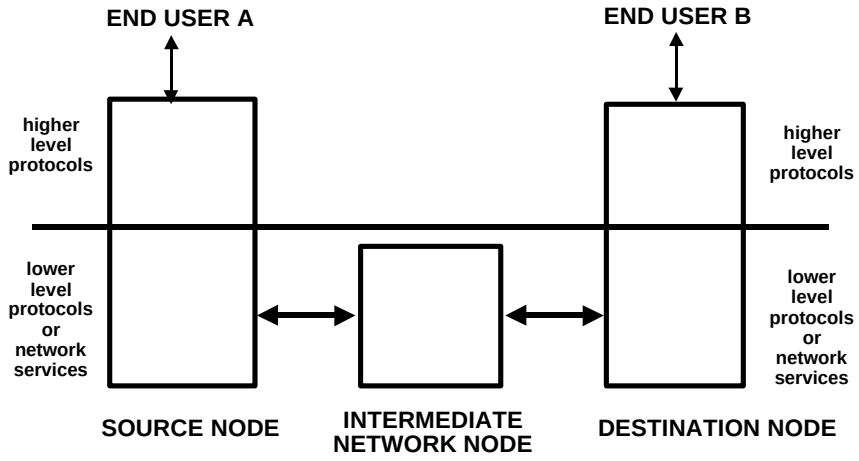
INTERNET ARCHITECTURE AND PROTOCOLS

OSI REFERENCE MODEL



22

OSI REFERENCE MODEL



23

TCP/IP PROTOCOL STACK BASIC PROTOCOLS

layer				
5-7	TELNET	FTP	SMTP	HTTP etc
4	TCP	UDP		
3	IP			
2	Ethernet	Token-Ring	ATM	PPP etc

24

TCP/IP PROTOCOL STACK BASIC PROTOCOLS

- **IP (Internet Protocol)**
  - **connectionless routing of packets**
- **UDP (User Datagram Protocol)**
  - **unreliable datagram protocol**
- **TCP (Transmission Control Protocol)**
  - **connection-oriented, reliable, transport protocol**

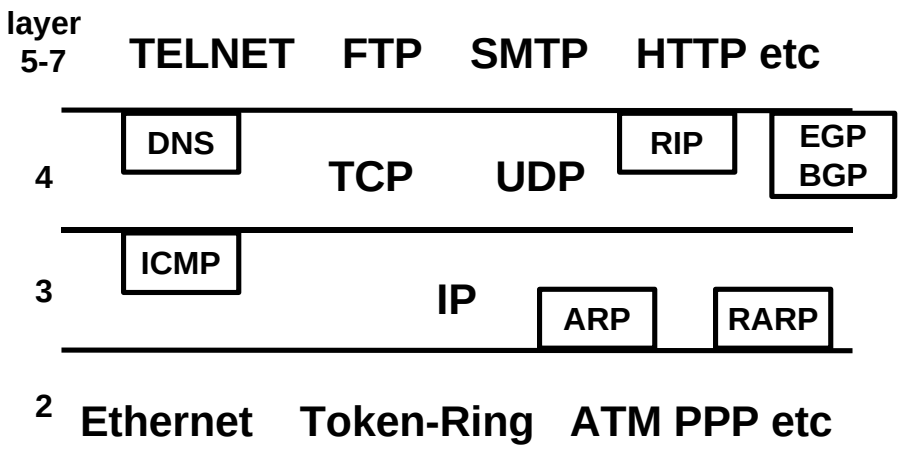
25

TCP/IP PROTOCOL STACK BASIC PROTOCOLS

- **TELNET: remote terminal**
- **FTP (File Transfer Protocol)**
- **TFTP (Trivial File Transfer Protocol)**
- **SMTP (Simple Mail Transfer Protocol)**
- **RPC (Remote Procedure Call)**
- **HTTP (Hyper Text Transfer Protocol)**
- **and others**

26

TCP/IP PROTOCOL STACK INFRASTRUCTURE PROTOCOLS



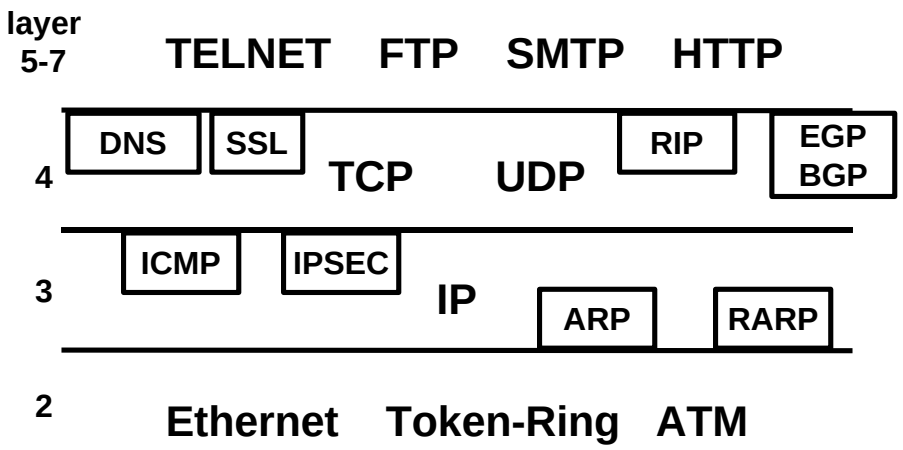
27

TCP/IP PROTOCOL STACK INFRASTRUCTURE PROTOCOLS

- **ICMP: Internet Control Message Protocol**
- **ARP: Address Resolution Protocol**
- **RARP: Reverse Address Resolution Protocol**
- **DNS: Domain Name Service**
- **RIP: Routing Information Protocol**
- **BGP: Border Gateway Protocol**
- **EGP: External Gateway Protocol**

28

TCP/IP PROTOCOL STACK SECURITY PROTOCOLS



29

INTERNET STANDARDS PROCESS

- **IETF: Internet Engineering Task Force**
  - **Application Area**
  - **General Area**
  - **Internet Area**
  - **Operational Requirements Area**
  - **Routing Area**
  - **Security Area**
  - **Transport Area**
  - **User Services Area**

30

IETF SECURITY AREA ACTIVE WORKING GROUPS

- IP Security Protocol (IPSEC)
- Transport Layer Security (TLS)
- Secure Shell (SECSH)
- Public Key Infrastructure X.509 (PKIX)
- Domain Name System Security (DNSSEC)
- S/MIME Mail Security (SMIME)
- Simple Public Key Infrastructure (SPKI)
- Common Authentication Technology (CAT)
- Web Transaction Security (WTS)
- One Time Password Authentication (OTP)
- Authenticated Firewall Traversal (AFT)
- An Open Specification for Pretty Good Privacy (OPENPGP)

31

RFCs AND IETF DRAFTS

- RFCs
  - Standards
    - Proposed Standard
    - Draft Standard
    - Internet Standard
  - Informational
  - Experimental
  - Historic
- IETF drafts
  - work in progress
  - expire after 6 months

32

MUST, SHOULD, MAY

- **MUST**
  - **mandatory, required of compliant implementations**
- **SHOULD**
  - **strongly recommended but not required**
- **MAY**
  - **possibility**
  - **even if not stated a may is always allowed unless it violates MUST NOT**

TCP/IP VULNERABILITIES

BASIC TCP/IP VULNERABILITIES

- many dangerous implementations of protocols
  - sendmail
- many dangerous protocols
  - NFS, X11, RPC
  - many of these are UDP based

35

BASIC TCP/IP VULNERABILITIES

- solution
  - allow a restricted set of protocols between selected external and internal machines
  - otherwise known as firewalls

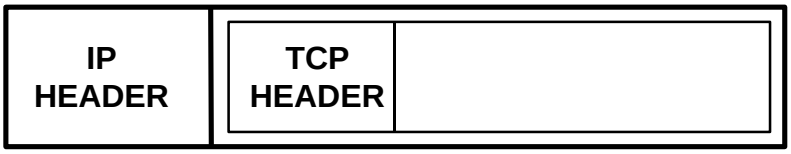
36

IP PACKET

- header
- data
  - carries a layer 4 protocol
    - TCP, UDP
  - or a layer 3 protocol
    - ICMP, IPSEC, IP
  - or a layer 2 protocol
    - IPX, Ethernet, PPP

37

TCP INSIDE IP



38

IP HEADER FORMAT

- **version: 4bit, currently v4**
- **header length: 4 bit, length in 32 bit words**
- **TOS (type of service): unused**
- **total length: 16 bits, length in bytes**
- **identification, flags, fragment offset: total 16 bits used for packet fragmentation and reassembly**
- **TTL (time to live): 8 bits, used as hop count**
- **Protocol: 8 bit, protocol being carried in IP packet, usually TCP, UDP but also ICMP, IPSEC, IP, IPX, PPP, Ethernet**
- **header checksum: 16 bit checksum**
- **source address: 32 bit IP address**
- **destination address: 32 bit IP address**

IP HEADER FORMAT

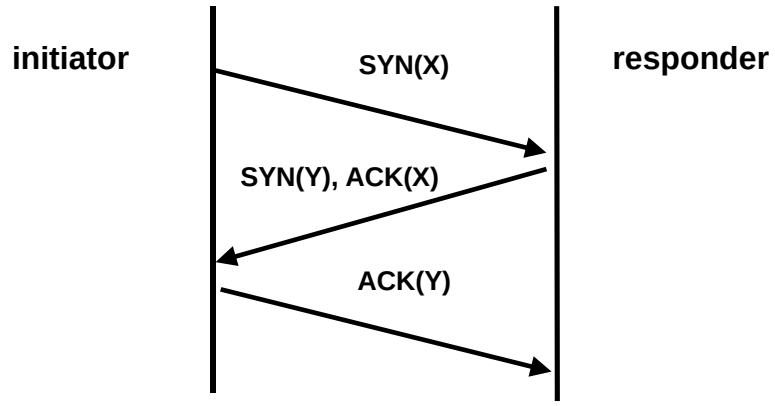
- **options**
  - **source routing**
    - **enables route of a packet and its response to be explicitly controlled**
  - **route recording**
  - **timestamping**
  - **security labels**

TCP HEADER FORMAT

- source port number
  - source IP address + source port number is a socket: uniquely identifies sender
- destination port number
  - destination IP address + destination port number is a socket : uniquely identifies receiver
- SYN and ACK flags
- sequence number
- acknowledgement number

41

TCP 3 WAY HANDSHAKE



42

TCP SYN FLOODING ATTACK

- **TCP 3 way handshake**
  - **send SYN packet with random IP source address**
  - **return SYN-ACK packet is lost**
  - **this half-open connection stays for a fairly long time out period**
- **Denial of service attack**
- **Basis for IP spoofing attack**

43

IP SPOOFING

- **Send SYN packet with spoofed source IP address**
- **SYN-flood real source so it drops SYN-ACK packet**
- **guess sequence number and send ACK packet to target**
  - **target will continue to accept packets and response packets will be dropped**

44

TCP SESSION HIJACKING

- Send RST packet with spoofed source IP address and appropriate sequence number to one end
- SYN-flood that end
- send ACK packets to target at other end

45

SMURF ATTACK

- Send ICMP ping packet with spoofed IP source address to a LAN which will broadcast to all hosts on the LAN
- Each host will send a reply packet to the spoofed IP address leading to denial of service

46

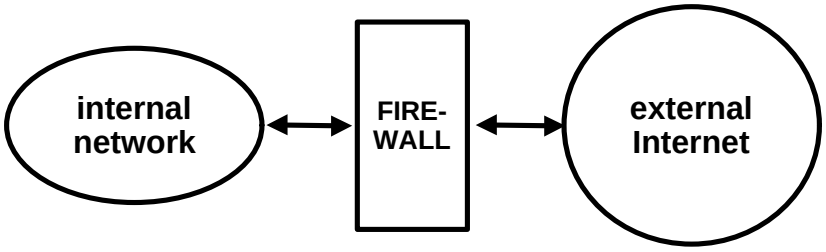
ULTIMATE VULNERABILITY

- IP packet carries no authentication of source address
- IP spoofing is possible
  - IP spoofing is a real threat on the Internet
  - IP spoofing occurs on other packet-switched networks also, such as Novell's IPX
- Firewalls do not solve this problem
- Requires cryptographic solutions

47

FIREWALLS

WHAT IS A FIREWALL?



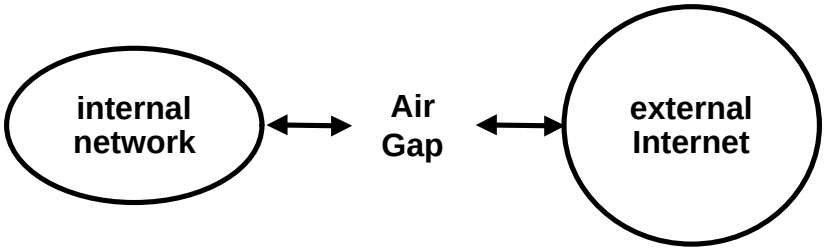
49

WHAT IS A FIREWALL?

- all traffic between external and internal networks must go through the firewall
  - easier said than done
- firewall has opportunity to ensure that only suitable traffic goes back and forth
  - easier said than done

50

ULTIMATE FIREWALL



51

BENEFITS

- secure and carefully administer firewall machines to allow controlled interaction with external Internet
- internal machines can be administered with varying degrees of care
- does work

52

BASIC LIMITATIONS

- connections which bypass firewall
- services through the firewall introduce vulnerabilities
- insiders can exercise internal vulnerabilities
- performance may suffer
- single point of failure

53

TYPES OF FIREWALLS

- Packet filtering firewalls
  - IP layer
- Application gateway firewalls
  - Application layer
- Circuit relay firewalls
  - TCP layer
- Combinations of these

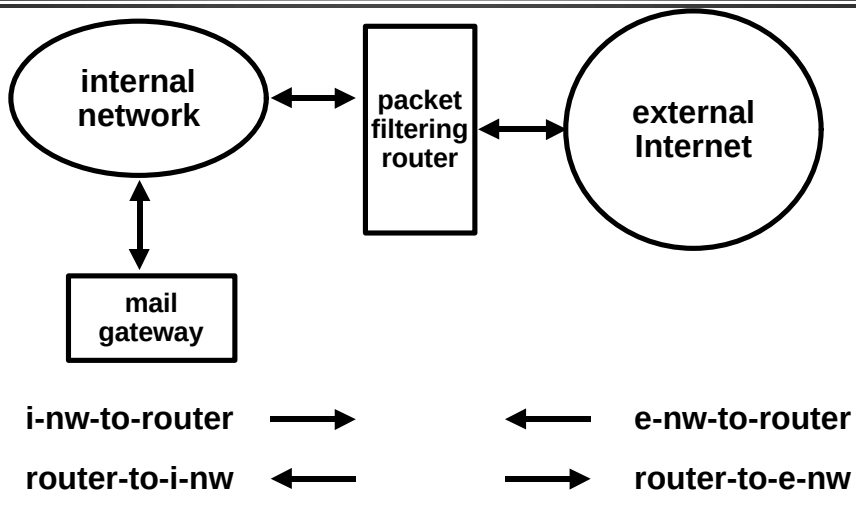
54

PACKET FILTERING FIREWALLS

- IP packets are filtered based on
  - source IP address + source port number
  - destination IP address + destination port number
  - protocol field: TCP or UDP
  - TCP protocol flag: SYN or ACK

55

FILTERING ROUTERS



56

PACKET FILTERING FIREWALLS

- drop packets based on filtering rules
- static (stateless) filtering
  - no context is kept
- dynamic (statefull) filtering
  - keeps context

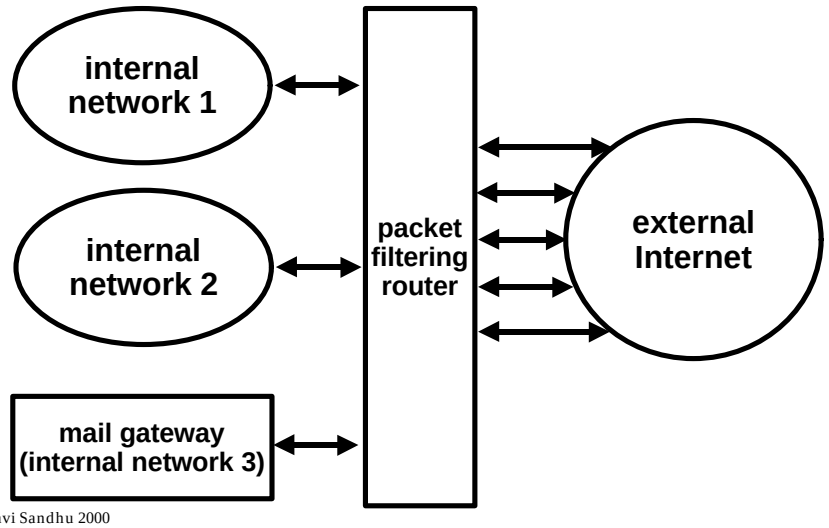
57

PACKET FILTERING FIREWALLS

- Should never allow packet with source address of internal machine to enter from external internet
- Cannot trust source address to allow selective access from outside

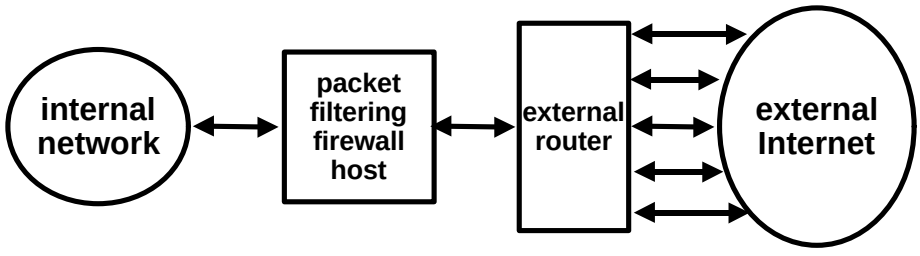
58

FILTERING ROUTERS



59

FILTERING HOST



- one can use a packet filtering firewall even if connection to Internet is via an external service provider

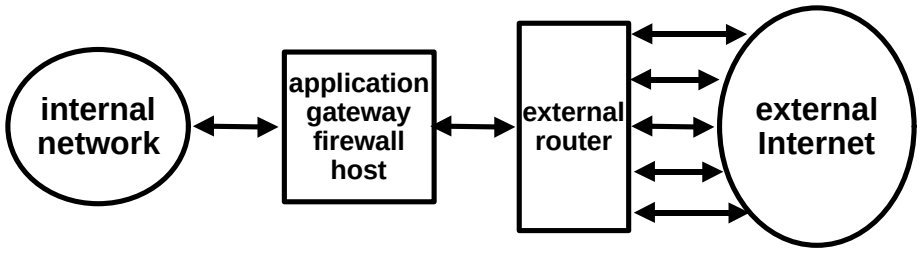
60

PACKET FILTERING FIREWALLS

- packet filtering is effective for coarse-grained controls
- not so effective for fine-grained control
  - can do: allow incoming telnet from a particular host
  - cannot do: allow incoming telnet from a particular user

61

APPLICATION GATEWAY FIREWALLS



SIMPLEST CONFIGURATION

62

APPLICATION PROXIES

- **have to be implemented for each service**
- **may not be safe (depending on service)**

63

CLIENT-SIDE PROXIES
Internal-Client External-Server

- **allow outgoing http for web access to external machines from internal users**
- **requires some client configuration**

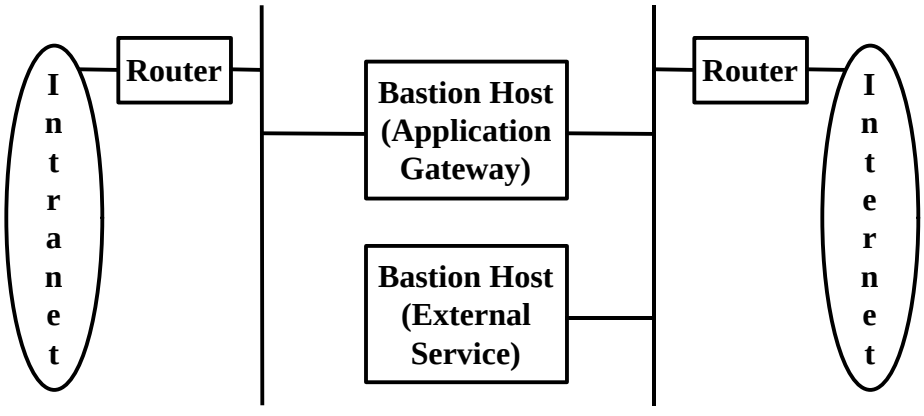
64

SERVER-SIDE PROXIES
External-Client Internal-Server

- allow incoming telnet for access to selected internal machines from selected external users
- requires some cryptographic protection to thwart sniffing and IP spoofing
- becoming increasingly important for
  - electronic commerce
  - VPN
  - remote access security

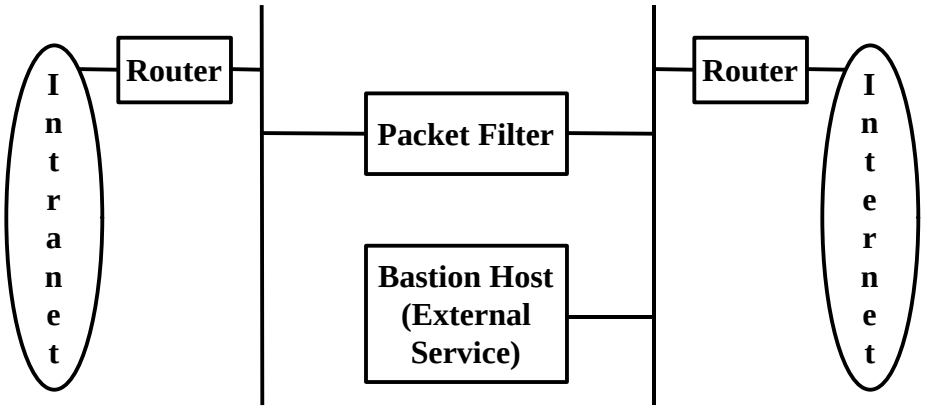
65

FIREWALL ARCHITECTURES
DUAL HOMED HOST



66

FIREWALL ARCHITECTURES SCREENED SUBNET



67

INTRUSION DETECTION

RELATED TECHNOLOGIES

- Intrusion detection
- Vulnerability assessment
- Incident response
- Honey pots
- Sniffer probes

69

INTRUSION DETETCION TECHNIQUES

- Policy detection (or knowledge-based)
  - default permit
    - attack-signature based detection
    - also called misuse detection
  - default deny
    - specification-based detection
- Anomaly detection (or behavior-based)
    - requires user profiling
    - requires some learning capability in the system
- Combinations of these

70

INTRUSION DETECTION DATA SOURCE

- network-based intrusion detection
  - multiple sensor points
- host-based intrusion detection
  - multi-host based
- application-based intrusion detection
- combinations of these

71

ATTACKER

- Outsider
  - easier
- insider
  - harder

72

INTRUSION DETECTION ISSUES

- **effectiveness**
- **efficiency**
- **security**
- **inter-operability**
- **ease of use**
- **transparency**

73

INTRUSION DETECTION CHALLENGES

- **False alarm rate**
- **Performance and scalability**

74

BASE RATE FALLACY

- Test for a disease is 99% accurate
  - 100 disease-free people tested, 99 test negative
  - 100 diseased people tested, 99 test positive
- Prevalence of disease is 1 in 10,000
- Alice tests positive
- What is probability Alice has the disease?

75

BASE RATE FALLACY

- Test for a disease is 99% accurate
  - 100 disease-free people tested, 99 test negative
  - 100 diseased people tested, 99 test positive
- Prevalence of disease is 1 in 10,000
- Alice tests positive
- What is probability Alice has the disease?

  1 in 100
- False alarm rate: 99 in 100 !!!!!

76

BASE RATE FALLACY BAYE'S THEOREM

- **population: 1,000,000**
- **diseased: 100**
- **disease free: 999,900**
- **false positive: 9,999**
- **true positive: 99**
- **Alice's chance of disease: 99/(9,999+99) = 1/100**

77

BASE RATE FALLACY 99.99% ACCURACY

- **population: 1,000,000**
- **diseased: 100**
- **disease free: 999,900**
- **false positive: 99.99**
- **true positive: 99.99**
- **Alice's chance of disease: 99.99/(99.99+99.99) = 1/2**

78

NETWORK-BASED INTRUSION DETECTION SIGNATURES

- **port signatures**
- **header signatures**
- **string signatures**

79

NETWORK-BASED INTRUSION DETECTION ADVANTAGES

- **Complements firewalls**
- **broad visibility into network activity**
- **no impact on network performance**
- **transparent installation**

80

NETWORK-BASED INTRUSION DETECTION DISADVANTAGES

- **False positives**
- **miss new unknown attacks**
- **scalability with high-speed networks**
- **passive stance**
- **emergence of switched Ethernet**

81

HOST-BASED INTRUSION DETECTION

- **host wrappers or personal firewalls**
  - **look at all network packets, connection attempts, or login attempts to the monitored machine**
    - **example, tcp-wrapper**
- **host-based agents**
  - **monitor accesses and changes to critical system files and changes in user privilege**
    - **example, tripwire**

82

INTRUSION DETECTION STANDARDS

- None exist
- ongoing efforts
  - CIDF: common intrusion detection framework
    for sharing information
  - IETF Intrusion Detection Working Group
    just started

INTRUSION DETECTION

- Needs to integrate with other security technologies such as cryptography and access control
- one component of defense-in-depth layered security strategy
- incident-response and recovery are important considerations