INFS 766
Internet Security Protocols

Lectures 1 and 2
Firewalls

Prof. Ravi Sandhu

OPENING REMARKS

COURSE PREREQUISITE

- **Must have completed INFS 612 or equivalent**
  - **concurrent enrollment in INFS 612 does not satisfy prerequisite**
- **Must be familiar with Discrete Mathematics and Formal Notation (such as INFS 501)**
- **INFS 762 is not required as a prerequisite**
- **Must be internet, web and pdf capable**
- **This is a protocols-oriented course**
  - **without these prerequisites you will have a hard time and will get no sympathy from me**

CONTACT INFORMATION

- **Prof. Ravi Sandhu**
  - **Professor of Information and Software Engineering** http://www.ise.gmu.edu
  - **Director, Laboratory for Information Security Technology (LIST)** http://www.list.gmu.edu
- **office: room 457, Science and Technology II**
  - **office hours: by appointment**
  - **email:** sandhu@gmu.edu
  - **voice: 703 993 1659**
  - **fax: 703 993 1638**
- **class web page:** http://www.list.gmu.edu/~infs766
- **class email:** infs766@list.gmu.edu
  - **for web page complaints**

SCHEDULE OF CLASSES

01/17/01	1	Firewalls
01/24/01	2	Firewalls
01/31/01	–	
02/07/01	3	Cryptography
02/14/01	4	Cryptography
02/21/01	5	SSL
02/28/01	**exam 1**	**lectures 1-5**
03/07/01	–	Spring Break
03/14/01	6	Digital Certificates
03/21/01	7	IPSEC
03/28/01	8	IPSEC
04/04/01	9	Kerberos
04/11/01	–	no lecture
04/18/01	10	Radius, OCSP
04/25/01	11	Secure Email
05/02/01	**exam 2**	**lectures 7-12**

COURSE MATERIAL

- **No text book**
  - **any book is already long obsolete**
- **Lecture slides are posted on the class web site in pdf format**
- **Class web site is not guaranteed to be available 24X7**

GRADING

- **Two in-class closed book exams**
- **Equal weightage**
- **Each lecture is important**

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

WEB SOURCES

- **source for RFCs and IETF**
  - **http://www.ietf.org**
- **cryptographic sources**
  - **RSA's frequently asked questions: http://www.rsasecurity.com/rsalabs/faq/index.html**
  - **NIST encryption home page: http://csrc.nist.gov/encryption/**
- **firewall sources**
  - **Firewalls frequently asked questions: http://www.interhack.net/pubs/fwfaq/**

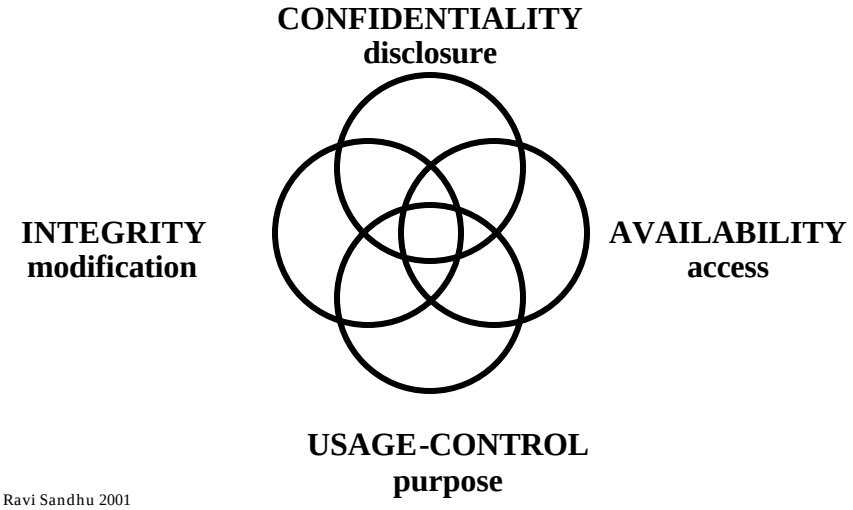
SECURITY COURSES CYCLE

- **Fall**
  - **INFS 762 Information Systems Security**
  - **INFS 767 Secure Electronic Commerce**
- **Spring**
  - **INFS 766 Internet Security Protocols**
  - **INFS 765 Database & Distributed Sys. Security**

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**
  - **Distributed denial of service attacks 2000**
- **Internet insecurity grows at super-Internet speed**
  - **security incidents are growing faster than the Internet (which has roughly doubled every year since 1988)**

SECURITY OBJECTIVES



SECURITY TECHNIQUES

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

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**

RISK

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

PERSPECTIVE ON SECURITY

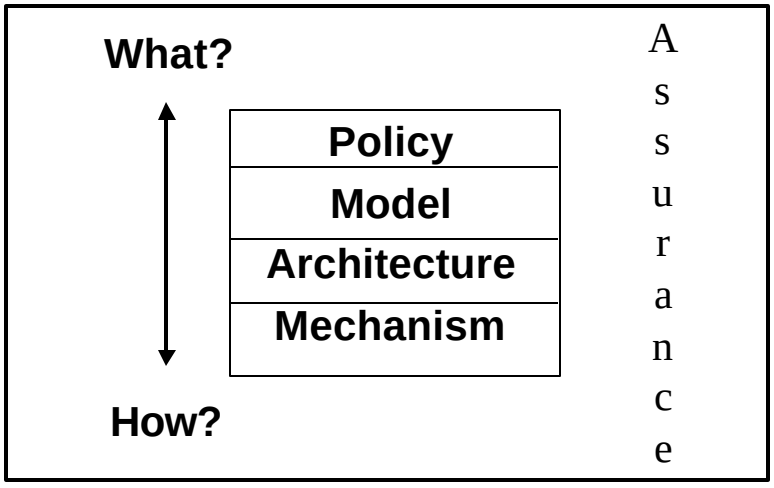
- **No silver bullets**
- **A process NOT a turn-key product**
- **Requires a conservative stance**
- **Requires defense-in-depth**
- **A secondary objective**
- **Absolute security does not exist**

- **Security in most systems can be improved**

PERSPECTIVE ON SECURITY

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

ENGINEERING AUTHORITY & TRUST 4 LAYERS



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**

CLASSICAL INTRUSIONS SCENARIO 2

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

NETWORK INTRUSIONS SCENARIO 3

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

DENIAL OF SERVICE ATTACKS

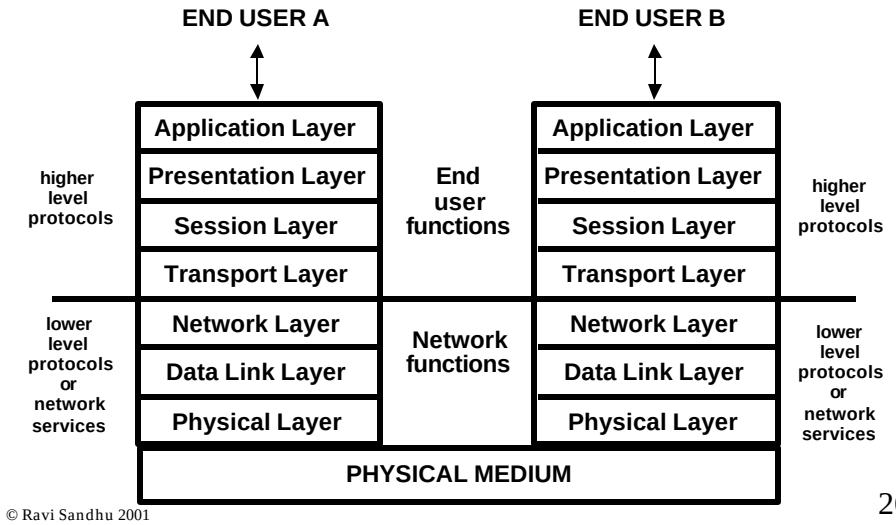
- **Flooding network ports with attack source masking**
- **TCP/SYN flooding of internet service providers in 1996**

INFRASTRUCTURE ATTACKS

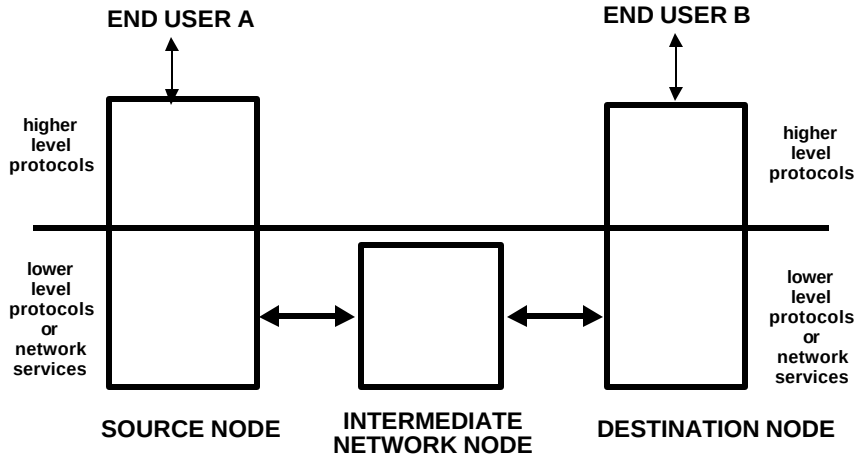
- **router attacks**
  - **modify router configurations**
- **domain name server attacks**
- **internet service attacks**
  - **web sites**
  - **ftp archives**

INTERNET ARCHITECTURE AND PROTOCOLS

OSI REFERENCE MODEL



OSI REFERENCE MODEL



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

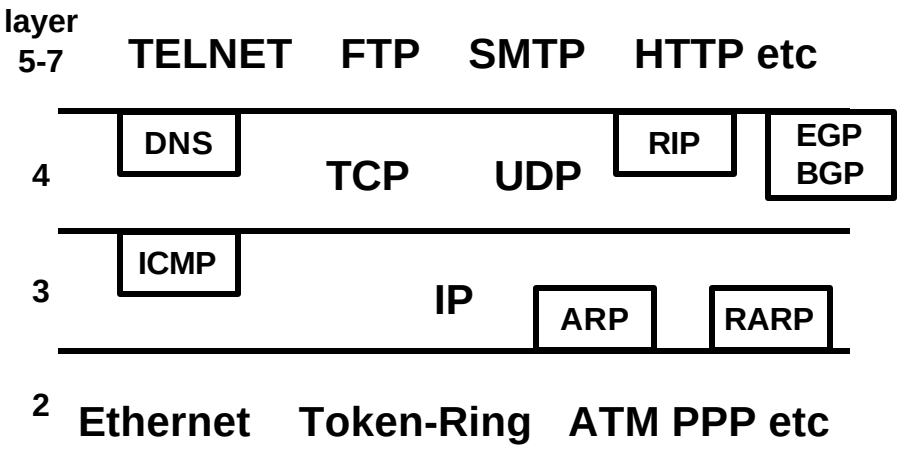
TCP/IP PROTOCOL STACK
BASIC PROTOCOLS

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

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**

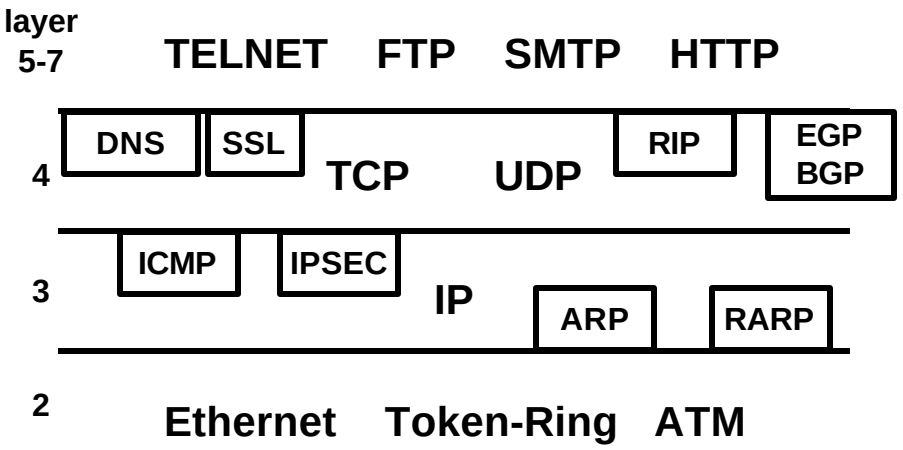
TCP/IP PROTOCOL STACK INFRASTRUCTURE PROTOCOLS



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**

TCP/IP PROTOCOL STACK SECURITY PROTOCOLS



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**

IETF SECURITY AREA ACTIVE WORKING GROUPS

- An Open Specification for Pretty Good Privacy (openpgp)
- Authenticated Firewall Traversal (aft)
- Common Authentication Technology (cat)
- IP Security Policy (ipsp)
- IP Security Protocol (ipsec)
- IP Security Remote Access (ipsra)
- Intrusion Detection Exchange Format (idwg)
- Kerberized Internet Negotiation of Keys (kink)
- Kerberos WG (krb-wg)
- One Time Password Authentication (otp)
- Public-Key Infrastructure (X.509) (pkix)
- S/MIME Mail Security (smime)
- Secure Network Time Protocol (stime)
- Secure Shell (secsh)
- Securely Available Credentials (sacred)
- Security Issues in Network Event Logging (syslog)
- Simple Public Key Infrastructure (spki)
- Transport Layer Security (tls)
- Web Transaction Security (wts)
- XML Digital Signatures (xmldsig)

RFCs AND IETF DRAFTS

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

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**

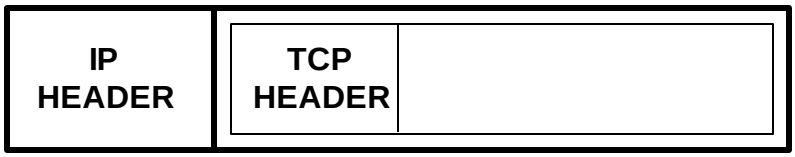
BASIC TCP/IP VULNERABILITIES

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

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**

TCP INSIDE IP



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**

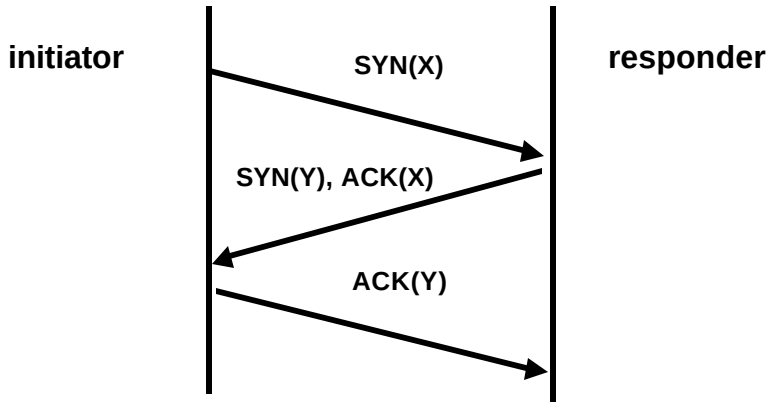
IP HEADER FORMAT

- **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**

TCP 3 WAY HANDSHAKE



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**

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**

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**

SMURF ATTACK

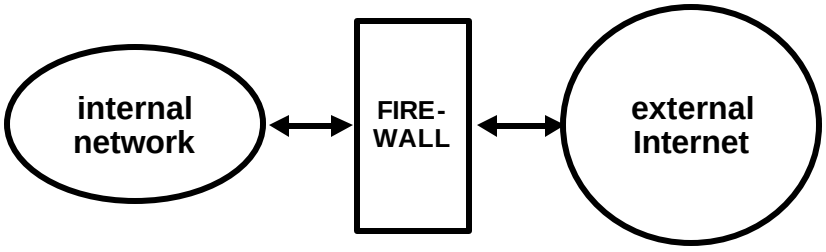
- **Send ICMP ping packet with spoofed IP source address to a LAN which will broadcast to all hosts on the LAN**
- **Each host will send a reply packet to the spoofed IP address leading to denial of service**

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**

FIREWALLS

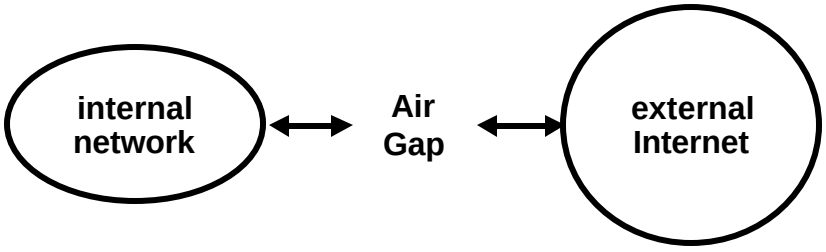
WHAT IS A FIREWALL?



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**

ULTIMATE FIREWALL



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**

BASIC LIMITATIONS

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

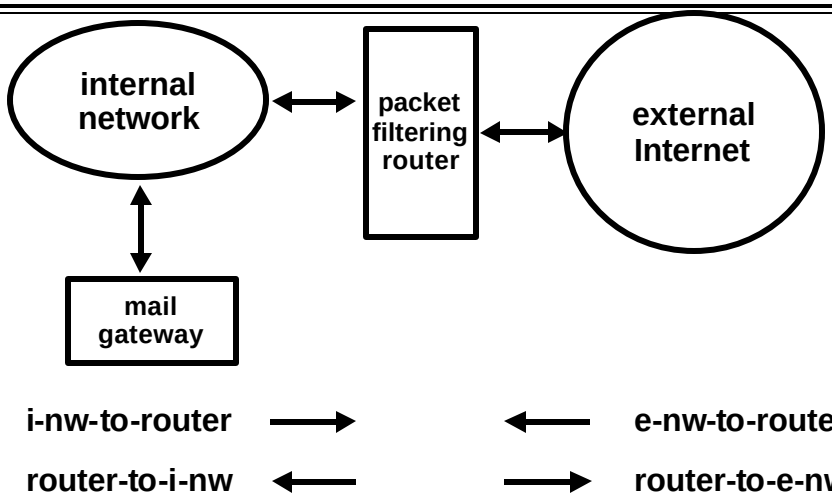
TYPES OF FIREWALLS

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

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**

FILTERING ROUTERS



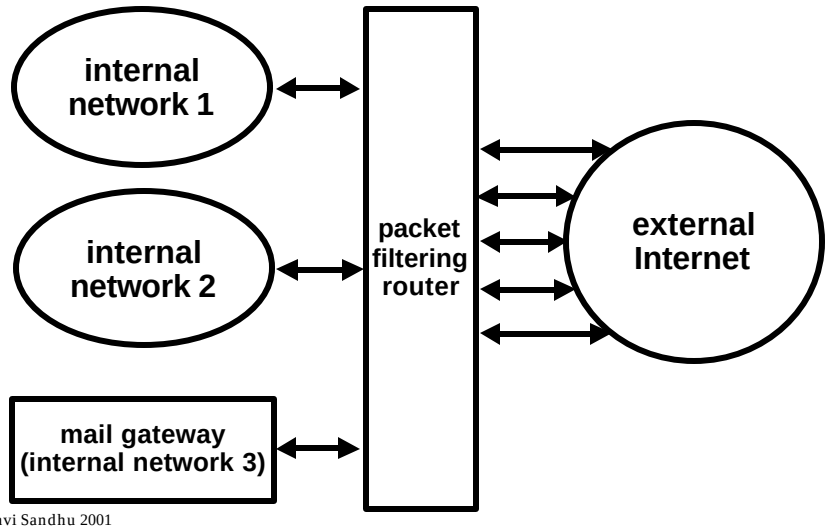
PACKET FILTERING FIREWALLS

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

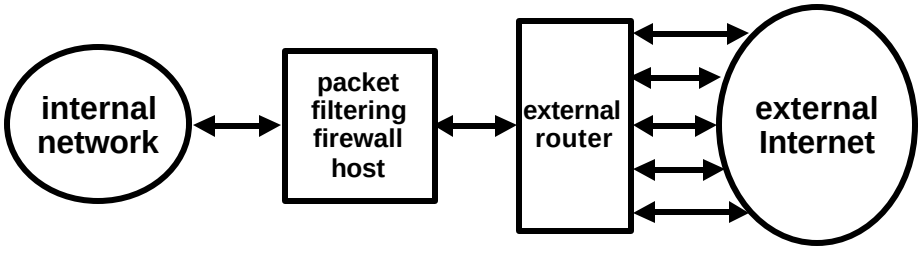
PACKET FILTERING FIREWALLS

- 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

FILTERING ROUTERS



FILTERING HOST

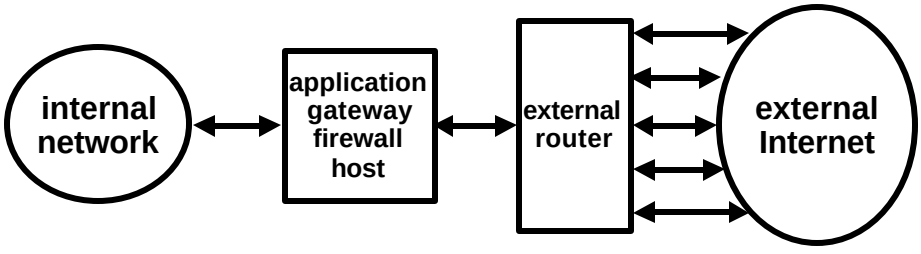


- one can use a packet filtering firewall even if connection to Internet is via an external service provider

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**

APPLICATION GATEWAY FIREWALLS



SIMPLEST CONFIGURATION

APPLICATION PROXIES

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

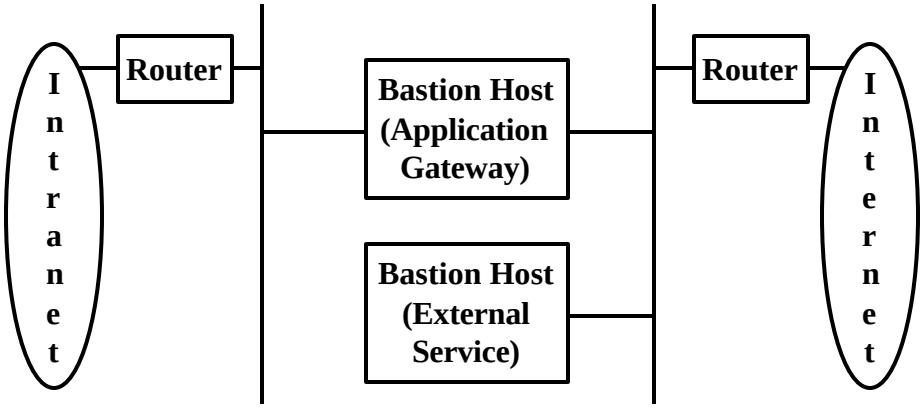
CLIENT-SIDE PROXIES
Internal-Client External-Server

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

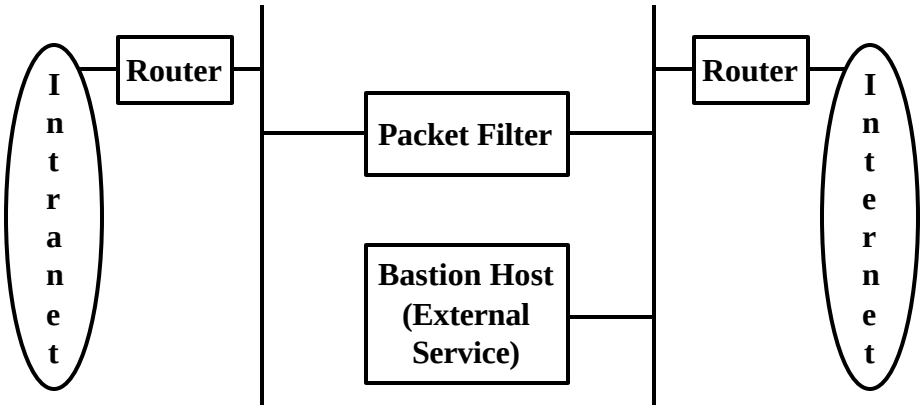
SERVER-SIDE PROXIES
External-Client Internal-Server

- **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**

FIREWALL ARCHITECTURES
DUAL HOMED HOST



FIREWALL ARCHITECTURES SCREENED SUBNET



INTRUSION DETECTION

RELATED TECHNOLOGIES

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

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**

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**

ATTACKER

- **Outsider**
  - **easier**
- **insider**
  - **harder**

INTRUSION DETECTION ISSUES

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

INTRUSION DETECTION CHALLENGES

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

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?**

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 !!!!!**

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**

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**

NETWORK-BASED INTRUSION DETECTION SIGNATURES

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

NETWORK-BASED INTRUSION DETECTION ADVANTAGES

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

NETWORK-BASED INTRUSION DETECTION DISADVANTAGES

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

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**

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