Network Security: Network Review and Firewalls

Henning Schulzrinne
Columbia University, New York
schulzrinne@cs.columbia.edu

Columbia University, Fall 2000

Last modified September 21, 2000

Slide 1

Secure Communications

- Alice can send message to Bob; only Bob can read
- Bob knows for sure that Alice sent it
- Alice can't deny she sent the message
- but the basic communication is insecure:
  - wiretapping
  - switches and routers
  - redirection
  - storage
  - ...
- $\leftrightarrow$ storage security

Slide 2

Security is analog, not binary. . .

- there is no perfect security
- cost of inconvenience vs. cost of breach
- how long does it have to stay secret?
- how sophisticated is the adversary?
- value of information + value of service (DOS)
- physical security + cryptographic
- difference: attack from anywhere, automated (“script kiddies”)
- most problems are not crypto problems
- wire/fiber-tapping is hard

Slide 3

Terminology

bad guy: avoid ‘hacker’; *Trudy* = intruder, impostor

secret key: = symmetric = receiver and transmitter share secret key, nobody else

public key: = asymmetric = two keys, one public, one private (secret)

privacy: protect communications from all but intended recipients $\approx$ confidentiality $\leftrightarrow$ privacy laws

Slide 4

Dramatis Personae

usually computers:

Alice: first participant

Bob, Carol, Dave: second, third, fourth participant

Eve: evesdropper

Mallory, Trudy: malicious active attacker

Trent: trusted arbitrator

Walter: warden; guarding Alice and Bob in some protocols

Peggy: prover

Victor: verifier

Slide 5

Kaufman Notation

$\oplus$	ex-or, exclusive or
$\mid$	concatenation (e.g., ”joe” $\mid$ ”secret” = ”joesecret”
$K\{\text{message}\}$	encrypted with key K
$\{\text{message}\}_{\text{Bob}}$	encrypted with public key of Bob
$[\text{message}]_{\text{Bob}}$	signed by Bob = using his private key

Slide 6

Network Primer

layer	name	who	e.g.,	PDU
7	application	E-E	SMTP	message
6	presentation	E-E	MIME	
5	session	E-E	?	
4	transport	E-E	TCP	packet
3	network	router	IP	packet
2	data link	bridge, switch	Ethernet	frame
1	physical	repeater	Ethernet over coax	bit stream

Slide 7

Network Services

(Almost) any layer:

error checking: checksum, drop bad packets

reliability: retransmission (ARQ, ”ack”) or forward error correction (redundancy)

ordering: ensure delivery order

multiplexing: several upper-layer entities $\rightarrow$ one lower-layer entity (e.g.,: telephony)

inverse multiplexing: spread single message over several channels

flow control: avoid overrunning slow receiver

congestion control: avoid overrunning slow network

encryption, authentication: obviously…

Slide 8

Directory Services

- need (network-layer) address to communicate
- more memorable, different assignment:
  - unique identifier
  - locator
  - name (administrative, “John Smith”, www.)
- directory service: translation between addresses
- scalability ➠ tree, hiearchy
- e.g.,: clinton@whitehouse.gov
- needed for security: public key
- needs to be secured

Slide 9

Network Security Layers

Physical layer: blackening

Data link layer: wireless Ethernet encryption (802.11 WEP at 11 Mb/s), PPP authentication

Network layer: IPsec

Transport layer: secure socket layer (TLS, “https:”)

Application: email (PGP, S/MIME), x-over-TLS, HTTP authentication, SHTTP, Kerberos

infrastructure: DNS, routing, resource reservations, . . .

Slide 10

Security Approaches

- Application security
- OS security
- Network infrastructure security
- Procedural and operational security

Slide 11

Application Security

- application software security (e.g., buffer overruns)
- path encryption via secure application protocols (ssh)
- isolating critical applications on single-purpose hosts

Slide 12

Host/OS Security

- OS software integrity (most attacks on non-patched OS)
- user-level access control (AAA, tokens)
- block unneeded services (finger, ftp, DNS)
- path encryption via IPsec
- device-level access control (MAC, IP, DNS) in servers, routers, Ethernet switches
- e.g., host firewalling (such as TCP wrappers, IP chains)

Slide 13

Network Infrastructure Security

- service-blocking perimeter (port)
- device-ID perimeter (IP address)
- path encryption perimeter
- path isolation via routers and switches
- path isolation via separate infrastructure (“air gap”)

Slide 14

Procedural and Operational Security

- policies and education on safe computing practices
- desktop configuration management
- proactive probing for vulnerabilities
- intrusion detection

Slide 15

Top-level Domains

2 letters: countries
3 letters: independent of geography (except edu, gov, mil)

domain	usage	example	domains (8/00)
com	business (global)	research.att.com	17,050,817
edu	U.S. 4 yr colleges	cs.columbia.edu	5,673
gov	U.S. non-military gov't	whitehouse.gov	730
mil	U.S. military	arpa.mil	
org	non-profit orgs (global)	www.ietf.org	248,489
net	network provider	nis.nsf.net	2,806,721
us	U.S. geographical	ietf.cnri.reston.va.us	
uk	United Kingdom	cs.ucl.ac.uk	194,686
de	Germany	fokus.gmd.de	262,708

Slide 16

Replicated Services

- load sharing
- availability
- same information?
- replay: change password to different server

Slide 17

Packet Switching

- circuit switching: fixed-rate, reserved bit stream between parties for duration of communications (“wire”)
- packet switching: chop application messages into packets ($<$ few kB, with upper bound):
  - interleaving from different sources
  - error recovery on single unit
  - flexible bandwidth

➠ encryption on messages or packets

Slide 18

Network Components

link: connection between components, including wireless ➠ point-to-point (modem), multiple access (Ethernet)

router, switch: forward packets

node: router (= intermediate system), host (= end system)

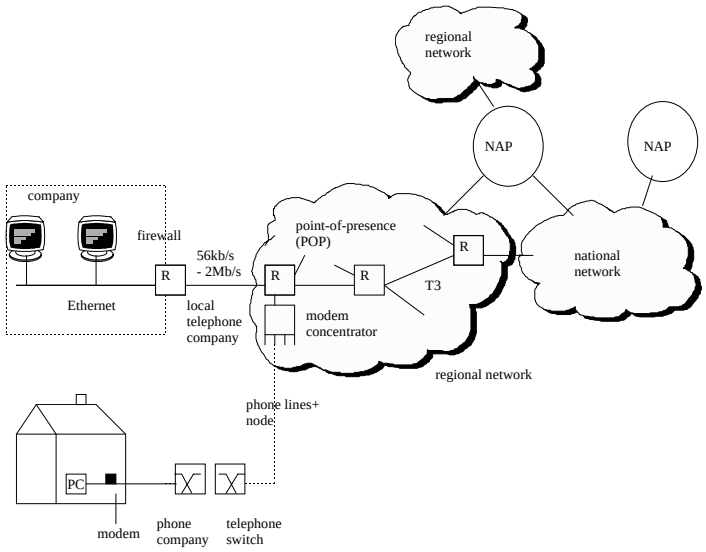
clients: access resources and services

servers: provide resources and services (may also be client)

dumb terminal: no local processing

Slide 19

Network Access and Interconnection



Slide 20

Destinations

- interconnect local networks (links) of different technology
- router:
  1. get packet from source link, strip link layer header
  2. find outgoing interface based on destination network address
  3. find next link-layer address
  4. wrap in link layer header and send

Slide 21

Internet Names and Addresses

	example	organization
MAC address	8:0:20:72:93:18	flat, permanent
IP address	132.151.1.35	topological (mostly)
Host name	www.ietf.org	hierarchical
User name	clinton@whitehouse.gov	multiple

host name $\overset{\mathrm{DNS,many-to-many}}{\rightarrow}$ IP address $\overset{\mathrm{ARP,1-to-1}}{\rightarrow}$ MAC address

addresses can be forged ➠ check source

Slide 22

Tempest

- every device is a radio transmitter
- e.g., TV scanning
- Europe: find unlicensed TV receivers
- *control zone*

Slide 23

Threats for a Corporate/Campus Network

- unauthorized access to hosts (clients, servers)
- disclosure & modification of network data
- denial-of-service attacks

Slide 24

Threats for the Internet/ISP

- propagate false routing entries (“black holes”, `www.citibank.com` $\longrightarrow$ `www.mybank.az`)
- domain name hijacking
- link flooding
- configuration changes (SNMP)
- packet intercept

Slide 25

Application-Layer Threats

- only limited ability of network intervention possible
- shoulder-surfing
- rogue applications emailing out confidential files
- viruses, mail bombs, email attachments, …

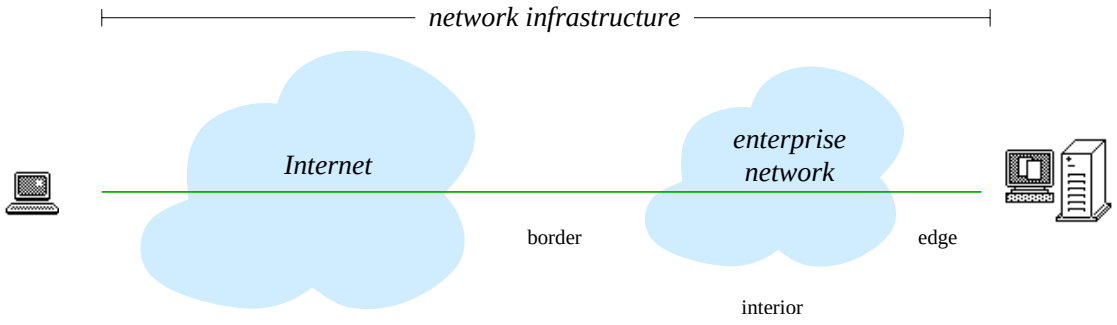
Slide 26

General Strategies

- hardening the OS and applications
- encrypting sensitive data
- reduce size of target $\longrightarrow$ disable unneeded services
- limit access of attacker to target systems

Slide 27

Network Infrastructure



Slide 28

Trust Model

- perimeter defense: defines *trust zone*
- most attacks are from the *inside*
- traveling users: virtual private networks – danger!
- “extranets” for vendors, suppliers, . . .
- internal hosts may not be managed or under control of network operator
- defense in depth

Slide 29

Firewalls

- computer between internal (“intranet”) and external network
- = policy-based packet filtering
- watch single point rather than every PC
- limit in/out services, restrict incoming packets
- can’t prevent people walking out with disks

packet filter: restrict IP addresses (*address filtering*), ports

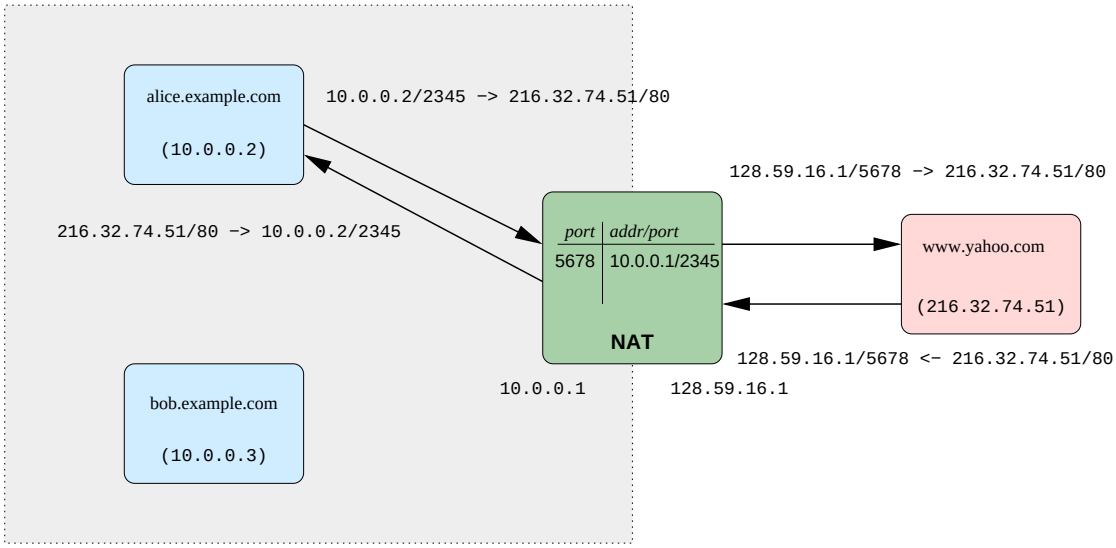
connection filter: only allow packets belonging to authorized (TCP) connections

encrypted tunnel: tunnel = layer same layer inside itself ➠ virtual network: connect intranets across Internet

NA(P)T: network address (and port) translator are *not* firewalls, but can prevent all incoming connections

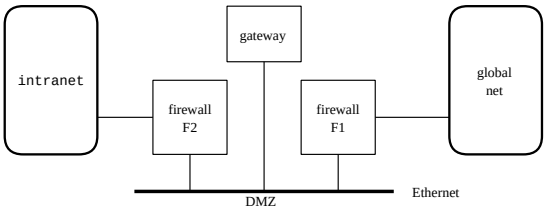
Slide 30

Network Address Translation



Slide 31

Application Gateway



- firewall F_x: only to/from gateway
- may only allow email, file transfer
- hard to restrict large file transfers

Slide 32

Key Escrow

- key broken into pieces, $\oplus$'ed
- need all key pieces ➠ need collusion
- doesn't prevent "bad guys" from using other cryptography
- useful in corporate environment: accidental key loss

Slide 33

Viruses

trojan horse: looks innocent, does something nasty

virus: inserts copy of itself into another program

worm: replicates across network

trapdoor: undocumented high-priviledge access to program

logic bomb: triggered at some time instant or event

Carriers:

- only programs ➠ "Good Times" hoax
- but: PostScript is program
- but: Word is a program

Slide 34

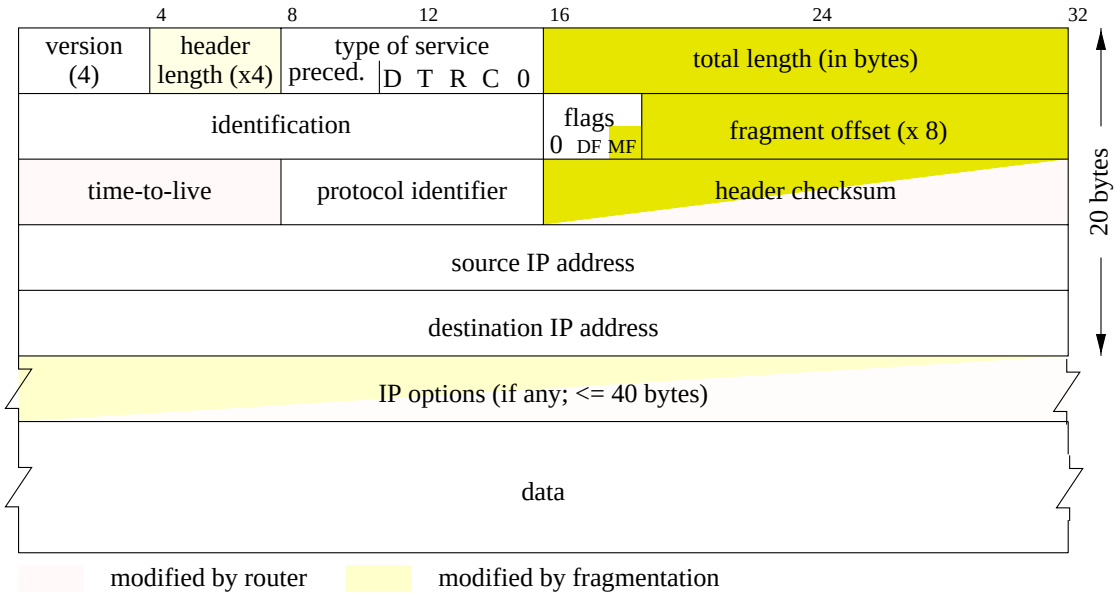
Virus Prevention

- signatures (➠ hash)
- but: polymorphic virus
- checksum files securely
- limit activity (*sandboxing*) ➠ Java
- run a non-Windows operating system …

also: some may do physical damage (EEPROM, tape, video monitor, speaker)

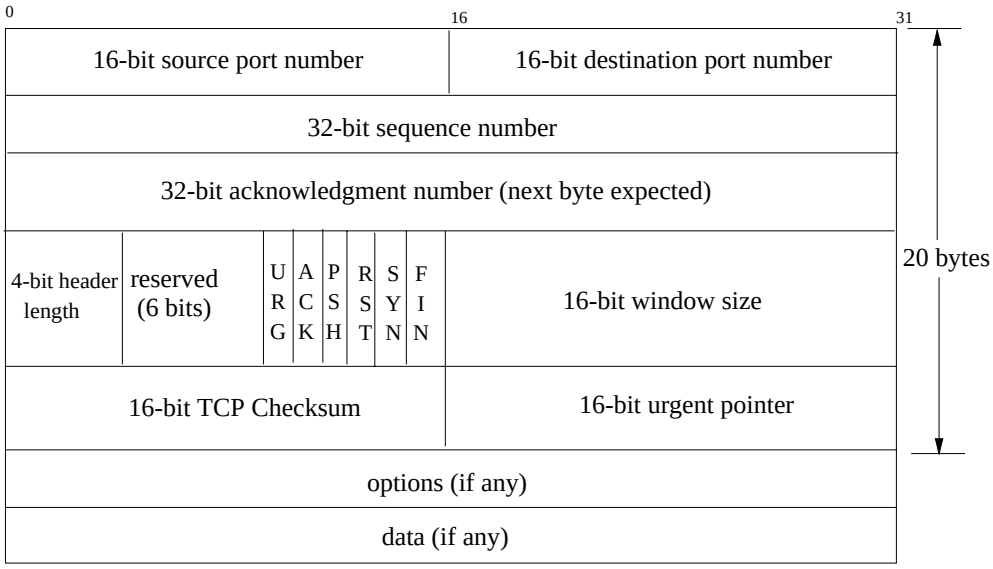
Slide 35

IPv4



Slide 36

TCP



Slide 37

Denial of Service (DOS) Attacks

Source: exploit legitimate behavior + bugs with “strange” packet formats.

mailbombing: send auto-generated email to victim

smurf: Perp sends ICMP echo (ping) traffic to IP broadcast address (directed broadcast), all of it having a spoofed source address of a victim. Prevention:

- disable directed broadcast;
- source address filtering on egress/ingress;
- compare source address of a packet against the routing table to ensure the return path of the packet is through the interface it was received on.
- “An ICMP Echo Request destined to an IP broadcast or IP multicast address MAY be silently discarded.”

fraggle: same, UDP echo packets;

Slide 38

LAND attack: spoofed packet(s) with the SYN flag set – if they contain the same destination and source IP address as the host, the victim's machine could hang or reboot;

Tear drop: overlapping (fragmented) packets;

SYN flood: send lots of TCP SYN packets that occupy OS resources;

crash server: large URLs, malformed packets, ...

Slide 39

Distributed Denial-of-Service Attacks

E.g.: Stacheldraht, Trinoo, Tribe Flood Network

- compromise victim system, typically via buffer overflow
- clients (control handlers via TCP), handlers (control agents via TPC or ICMP ECHO_REPLY), agents (send data)
- handler-to-agent communication is encrypted
- handlers instruct agents to start DOS:
  - SYN flood
  - ICMP flood
  - UDP flood
  - Smurf

Slide 40

Military Security Model

Access controls:

discretionary: owner gives out rights

nondiscretionary: policy fixed

- security levels: unclassified $<$ confidential $<$ secret $<$ top secret
- compartments ➠ "need to know"
- read up is illegal
- write down is illegal (➠ root can't write to user!)

Slide 41

Covert Channels

- smuggle information without detection, but with noise – "steganography"
- timing ➠ system loading
- (printer) queues
- create out-of-bounds file: can't read vs. doesn't exist
- error messages
- related application: additive "noise" in pictures, music, videos for fingerprinting (example: Secure Digital Music Initiative (SDMI), assumes trusted player)

Slide 42

Orange Book

- military security, linear, documentation/testing

  D: none

  C1: discretionary security (Unix); prevent OS writing

  C2: ACL, no dirty disks, auditing (e.g., Windows NT 4.0, Solaris 2.6)

  B1: security labels for users, processes, devices

  B2: avoid Trojan horse; security level change notification; security kernel; covert channels

  B3: ACL with exceptions; alarms; secure crashing

  A1: verified design

Slide 43

Legal Issues

Patents:

- interesting things are patented (17 years)
- but some are royalty-free (DES), at least for non-commercial use (IDEA)
- public key requires license (until 2000) from RSA (4,405,829, issued September 29, 1983)

Slide 44

Export Controls

Modified policy as of Jan. 2000

- classically, encryption = munitions
- book ok, disk not
- export license: DOD ➠ DOC for export to government
- no export to Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria
- technical review for export to non-government
- “retail products” can now be exported to any end user
- open source do not need review, but deposit source code
- $<$64 bit encryption (including DES) mostly o.k. for export (Wassenaar agreement)
- USA, Australia, New Zealand, France, and Russia control export
- import always ok

Slide 45