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
  - ...
- ↔ storage security
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

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
Dramatis Personae

usually computers:

Alice: first participant
Bob, Carol, Dave: second, third, fourth participant
Eve: eavesdropper
Mallory, Trudy: malicious active attacker
Trent: trusted arbitrator
Walter: warden; guarding Alice and Bob in some protocols
Peggy: prover
Victor: verifier

Kaufman Notation

⊕ ex-or, exclusive or
| concatenation (e.g., "joe" | "secret" = "joesecret"
K {message} encrypted with key K
{message} Bob encrypted with public key of Bob
[message] Bob signed by Bob = using his private key
Network Primer

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

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 → 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...
**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, hierarchy
- e.g.: clinton@whitehouse.gov
- needed for security: public key
- needs to be secured

**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, …
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)

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”)
Procedural and Operational Security

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

---

Top-level Domains

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

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

---

Slide 15

Slide 16
Replicated Services

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

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
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

Internet Names and Addresses

<table>
<thead>
<tr>
<th>example</th>
<th>organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC address</td>
<td>8:0:20:72:93:18</td>
</tr>
<tr>
<td>IP address</td>
<td>132.151.1.35</td>
</tr>
<tr>
<td>Host name</td>
<td><a href="http://www.ietf.org">www.ietf.org</a></td>
</tr>
<tr>
<td>User name</td>
<td><a href="mailto:clinton@whitehouse.gov">clinton@whitehouse.gov</a></td>
</tr>
</tbody>
</table>

addresses can be forged ➤ check source
Tempest

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

Threats for a Corporate/Campus Network

- unauthorized access to hosts (clients, servers)
- disclosure & modification of network data
- denial-of-service attacks
Threats for the Internet/ISP

- domain name hijacking
- link flooding
- configuration changes (SNMP)
- packet intercept

Application-Layer Threats

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

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

Network Infrastructure

- network infrastructure
  - Internet
  - enterprise network
    - border
    - edge
    - interior

Slide 27

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

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
Network Address Translation

16.0.0.2/2345 -> 216.32.74.51/80
216.32.74.51/80 -> 16.0.0.2/2345

port 5678 10.0.0.1/2345

128.59.16.1/5678 -> 216.32.74.51/80
128.59.16.1/5678 <= 216.32.74.51/80

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, "’ed
- need all key pieces ⇒ need collusion
- doesn’t prevent “bad guys” from using other cryptography
- useful in corporate environment: accidental key loss

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
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)

IPv4

Slide 35

<table>
<thead>
<tr>
<th>4</th>
<th>8</th>
<th>12</th>
<th>16</th>
<th>24</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>header length</td>
<td>type of service</td>
<td>total length (in bytes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(4)</td>
<td>(x4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>identification</td>
<td>flags</td>
<td>fragment offset (x 8)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>time-to-live</td>
<td>protocol identifier</td>
<td>header checksum</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>source IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>destination IP address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP options (if any; &lt;= 40 bytes)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Slide 36
**TCP**

<table>
<thead>
<tr>
<th>Field</th>
<th>Bit Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-bit source port number</td>
<td>0-15</td>
</tr>
<tr>
<td>16-bit destination port number</td>
<td>16-31</td>
</tr>
<tr>
<td>32-bit sequence number</td>
<td>32-47</td>
</tr>
<tr>
<td>32-bit acknowledgment number</td>
<td>48-63</td>
</tr>
<tr>
<td>4-bit header length</td>
<td>1</td>
</tr>
<tr>
<td>reserved (6 bits)</td>
<td>2-7</td>
</tr>
<tr>
<td>URG</td>
<td>8</td>
</tr>
<tr>
<td>ACK</td>
<td>9</td>
</tr>
<tr>
<td>PSH</td>
<td>10</td>
</tr>
<tr>
<td>RST</td>
<td>11</td>
</tr>
<tr>
<td>SYN</td>
<td>12</td>
</tr>
<tr>
<td>FIN</td>
<td>13</td>
</tr>
<tr>
<td>16-bit TCP Checksum</td>
<td>14-31</td>
</tr>
<tr>
<td>options (if any)</td>
<td>32-63</td>
</tr>
<tr>
<td>data (if any)</td>
<td>64-2048</td>
</tr>
<tr>
<td>16-bit window size</td>
<td>64-65</td>
</tr>
</tbody>
</table>

**Denial of Service (DOS) Attacks**

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

**mail bombing**: 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;
**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, ...

---

**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

---
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!)

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)
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

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)
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