SECURITY
- what does it mean?

CONFIDENTIALITY

– *Keep our data from prying eyes*

INTEGRITY

– *Protect our data from loss or unauthorised alteration*

CONTROL USE OF RESOURCES

– *Our expensive equipment is intended for our use only!*

MAINTAIN AVAILABILITY

– *Because users rely on our systems working properly*

Not just a network problem!

SECURITY IMPLICATIONS OF CONNECTING TO THE INTERNET

Internet lets you connect to millions of hosts...

– *but they can also connect to you!*

Many points of access (e.g. telephone, X25)

– *even if you can trace an attack to a point on the Internet, the real source may be untraceable*

Your host runs many Internet servers

– *many potential points of vulnerability*

– ***most servers run as 'root' !!***

AUTHENTICATION

We want to limit access to those who are genuinely authorised.

Each method has its own problems.

1. Passwords

- *can be guessed*
- *if sent unencrypted, can be "sniffed" from the network and reused*

2. Source IP address

- *not verified by network (since not used in datagram delivery)*
- *datagrams are easily forged*

3. Source host name

- *DNS is easily attacked (e.g. by loading false information into cache)*

AUTHENTICATION (contd)

4. Source port

– *used by rcp, rsh, rlogin… (BSD)*
– *relies on fact that under Unix, only 'root' can use source ports between 1 and 1023 (TCP & UDP)*
– *hackers can send forged datagrams from another O/S, e.g. DOS*
– *anybody can build their own Unix box and be 'root'*

5. Cryptographic methods

✓ *really secure solutions*
– *hard to implement, many tools, usually requires special clients*
– *export and usage restrictions*
– *keys can still be guessed if chosen by humans*

Note: some protocols perform virtually no authentication and are just plan INSECURE! (e.g. NFS, X11)

SECURITY HORROR STORIES

- **fingerd**

- **sendmail**
  (perennial!)

What to do? On your hosts…

1. *Limit the servers which are available; disable unused servers in* **/etc/inetd.conf**
2. *Limit access to specific hosts: "TCP Wrapper"*
3. *Don't connect to the Internet!*