April, 2005 -- Lecture 27

22C:169 Computer Security

Douglas W. Jones

Department of Computer Science

Network Threats II

IP Protocols - Inherently unprotected

IP address: 128.255.45.57:80

- 128.255 = *uiowa.edu*
- .45 = *division of math sciences (also 44)*
- .57 = *pyrite.cs.uiowa.edu*
- :80 = *my web server, if I had one*

The name space is exposed and public

Anyone can

- *scan the available address space*
- *attempt to connect to any port*

Classic IP Applications have no security

Example: mail (SMTP)

Open TCP session to port 25 and send:

```
MAIL FROM: <president@...>
RCPT TO: <jones@cs...>
DATA
<message body>
.
```

No authentication at all!

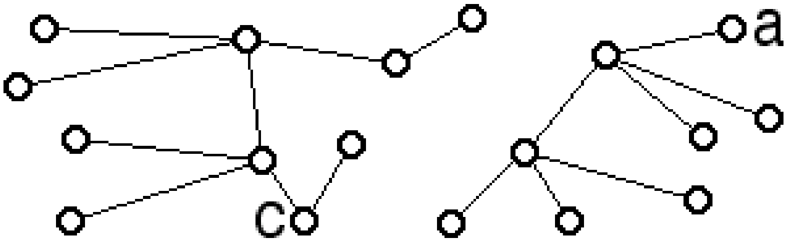
Anyone can use telnet to fake this!

Great for debugging or spamming!

Typical suggestion:

Don't connect your system to the net!

install an "air gap"



Now, no threat from c can reach a!

A is indeed protected.

Air gap is a term from power engineering

Air Gap Failures

How do you move data across an air gap?

you rarely want complete isolation!

Hand carry the data?

floppy disks, CF cards, microdrives?

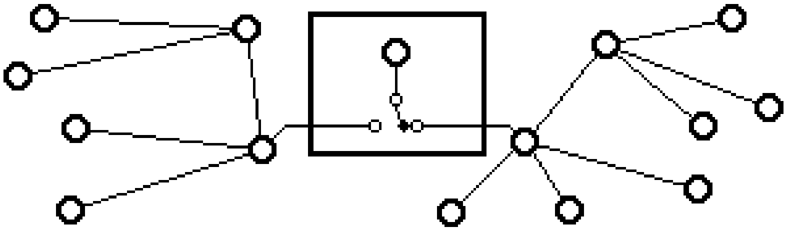
This is sneakernet technology

Can we stop covert sneakernet channels?

If media moves, how do we know it does not carry unauthorized content?

Air Gap Products

You can buy commercial air gap machines



The machine in the air gap may be

passive: just a disk or flash memory

active: a full network node

Evaluation of Air Gaps

When successful

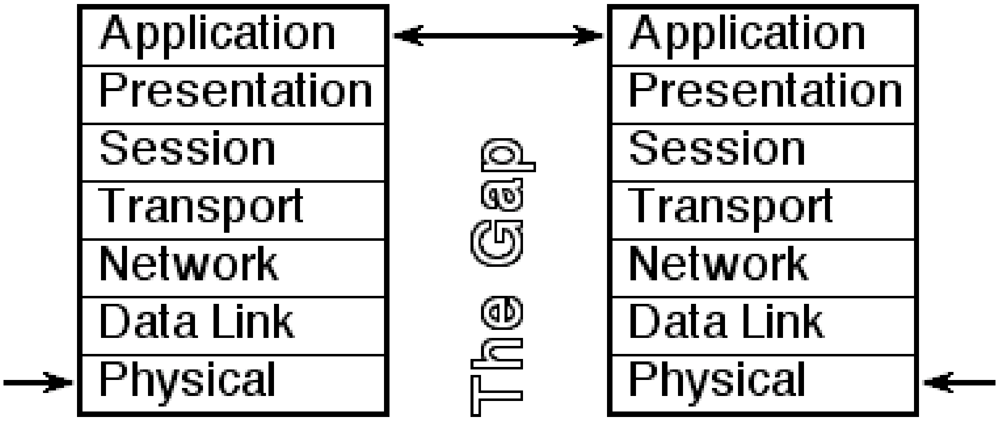
the applications on each side of air gap lift only permitted data over the gap

But air gaps offer no guarantees

an application can lift any data over the air gap. If the protocol stack is transparent, even raw network packets!

What matters is the application on each side, not the air gap itself.

In ISO-OSI terms:



What really matters?

Isolation of application to application communication from lower layers

Admission

Applications must have private presentation of a private data link layer using a private physical link.

Therefore

Local security is crucial

We want strong local operating systems

Ideally

Network layers below the applications should be isolated from any access to or knowledge of the gap crossing link

Common kluge

Use a link technology for which there is no known IP stack implementation.