Building a Real Session Layer

These slides are unfortunately, of little use.

Please see updated materials at fived.capelis.dj.

Please allow me to introduce myself

I'm me.

There.

Introduction Done!

Let's start at the beginning

(Everyone knows this part... but just let me quickly go through it.)

What's a Session Layer?

ISO 7 Layer Model

(Designed by committee)

1 – Physical Layer
(e.g. Cat 6, Fiber, Air)

2 – Data Link Layer
(e.g. Ethernet, 802.11[abgns...], FDDI)

3 – Network Layer
(Most commonly IP)

4 – Transport Layer
(e.g. TCP, UDP and a bunch of others)

5 – Session Layer
(Mostly unused)

6 – Presentation Layer
(Even more unused)

7 – Application Layer
(Everything)

So where's the application layer?

It kinda went everywhere....
(ewww... TWSS?)

Encryption:
SSL, SSH, IPSec (?)

Authentication:
Network services shouldn't have to ask.

See also: I want to use my SSH keys for everything and there's no good reason I shouldn't be able to!

Tons of service specific stuff that got pushed into the application layer

Generally each application is reimplementing some idea of a session independently.

More Code.

More Code. More Buggy Code.

So let's get rid of that while we're here.

Why do application multiplexing in layer 4?

I dunno.

Yoink

Layer five'd

Speaking of which...

That's what we're calling this software.

fived

Short for: Layer Five Daemon

Here's what we're going to put into fived:
Application Multiplexing
Authentication
Encryption

Things that go away:

Port Numbers

Port Knocking

Host Based Firewalls

Authentication
(Sometimes)

...

Really?

Yes... really.

No port numbers

Please do one of the following

If you're not with me on this... shout an expletive

If you're with me on this... loudly proclaim:
“Hmm... interesting”

Best thing about Defcon:

Having hundreds of people swear at you.

Moving on!

So let's take this slowly, in the order of most surprising to least

No port numbers

Precedence!

Portmapper

Do the same thing DNS did for IP addresses with port numbers

(What about SRV records?)

(Well... are you using them?)

(Likely answer: no)

Why not?

a) not every machine runs it's own DNS server

b) sysadmin doesn't always control DNS

c) a few other things

So what are we doing instead?

RFC 1078

Little known protocol called TCPMUX

Hey small bit of trivia!

Run this command on a unix box:
grep tcpmux /etc/services

Huh... it's got a reserved port number:

```
tcpmux          1/tcp
tcpmux          1/udp
```

I guess... I'll just have to go with that one then.

(*Maybe* that was half the inspiration for this project)

Wait... wait a second!

What about... inetd, xinetd and launchd

Well... sure.

But watch this:

Demos, Demos, Demos.

Questions?
Accusations?

http://fived.capelis.dj

For those of you on the conference CD...

These slides are totally terrible.

Please download a newer version from the website. (Defcon or mine.)