Building a Real Session Layer

D.J. Capelis
Defcon 16
Let's start at the beginning
It's easier to end at the end when you start at the beginning
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[abgnsv...], 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
(Usually made fun of)
7 – Application Layer (Everything)
So where's the session layer?
It kinda went everywhere....
Encryption:
SSL, SSH, IPSec (?)
Authentication:
Individual applications shouldn't be doing encryption
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.
So let's get rid of it
While we're here....
Why do application multiplexing in layer 4?
I dunno
Layer five'd
Speaking of which...
That's what we're calling this software.
fived
Short for: Layer Five Daemon
Current Development Status:
Don't actually run it
Useful for demos only
Here's what we're going to put into fived:
    Application Multiplexing
    Authentication
    Encryption
Things that go away:
Port Knocking
Host Based Firewalls
Authentication
(As much as possible)
Port Numbers
Really?
Yes... really.
No port numbers
If TCP/UDP hadn't done them, we'd have had a real session layer 20 years ago.
Okay, so... taking out port numbers, kind of a big deal
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. (If not at least a hundred of you swore, I'm disappointed in Defcon and standing on the stage looking a bit like an idiot right now)
Back to the topic at hand...
So let's take this slowly, in the order of most surprising to least
No port numbers
Precedence!
Portmapper
Does the same thing DNS did for IP addresses with port numbers. Kind of.
(What about SRV records?)
(Well... are you using them?)
(That's what I thought...)

Why not?
a) not every machine runs its own DNS server
b) sysadmin doesn't always control DNS
c) a few other things
You talk big... what's your solution?
RFC 1078
Little known protocol called TCPMUX
Celebrates its 20\textsuperscript{th} birthday in November
Very simple protocol
Entire specification is a paragraph
HELP provides a list of service names
Type service name, followed by CRLF
Server responds with + or – followed by optional message and CRLF
“Selected protocol starts”
(The RFC is completely silent on what happens after that or when the protocol ends)
So how does it help us with all the features I'm talking about?
It provides a sexy port number
Run this command on a unix box:
grep tcpmux /etc/services
tcpmux          1/tcp
tcpmux          1/udp
Since that's too good to pass up, we comply with the RFC
Protocol is extended via “services” that are built-in to fived and enable additional features
Built-ins (as of today)
HELP
Required by RFC, lists service names
AUTH
+ Success
Enter Username: demo
Enter Password: demopass
Authentication as demo successful
HOST
HOST
+ Success
Which VHOST? main
SSL
Does almost exactly what you think it does
MULTIPLEX
Allows you to layer as many layer 7 connections into our layer 5 connection as you want
Changes networking
Traditional Networking:
Your application connects to another application
With fived:
Your computer connects with another computer
Your applications use that session to communicate just as they do today
App <-> Session Client <-> fived <-> Service
Let's go ahead and see it
(Ignore the fact I don't have four different computers)
Demos, Demos, Demos.
Random Parting Thoughts

• IPv6 is sweet, you should all use it.
  – he.net and sixxs.net provide free tunnels
• Intel provides microcode updates for a reason, linux distros rarely do a good job of installing them or keeping up with the latest versions
• Firewalls are a poor man's substitute for security
• Security shouldn't be an excuse not to do things
For those of you with the conference CD...

Those slides are not the same as these.

Please download a newer version from the website.  (Defcon or mine.)
Questions?
Accusations?
(To be continued in Room 104)
Contact

Project:
http://fived.capelis.dj

Personal:
mail@capelis.dj
http://capelis.dj