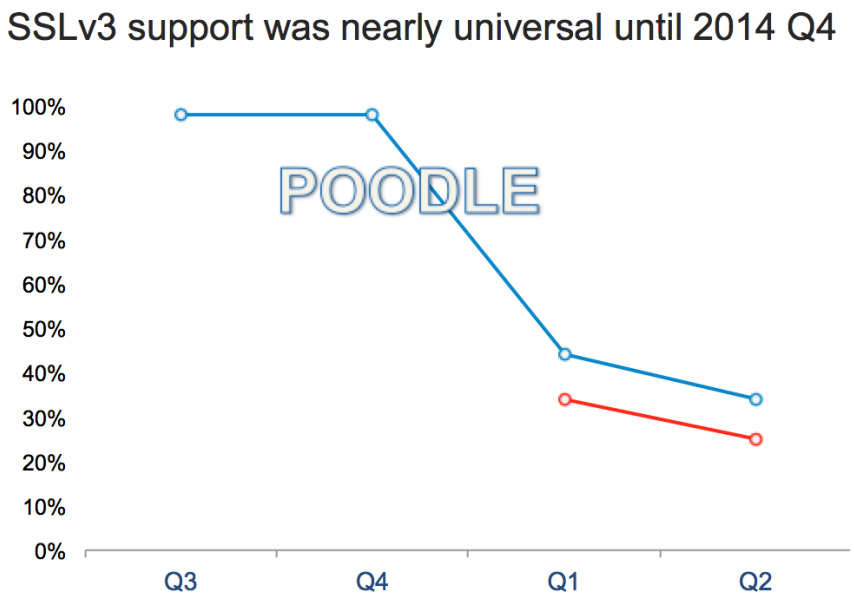
How much of my traffic is still SSLv3?

David Holmes, 2015-09-09

When the POODLE vulnerability came out in 2014, it was hailed as the death knell for SSL version 3. In the quarter just prior to POODLE, 98% of Internet sites supported SSLv3, but a year later that support had dropped to just 33%.



Blue: Internet at large. Red: F5 devices.

Even though the POODLE vulnerability was never seen as an exploit against servers in the wild, system administrators have been keen to increase their security posture against it. And, because of POODLE, Ivan Ristić's SSL labs system tester will no longer provide A grades to sites that support SSLv3.

So, customers have asked me, "Hey, David, can I disable SSLv3 yet?" My answer has been, "Yes, you can. *Unless* you still have a lot of SSLv3 traffic. Do you?"

And then they yelled, "WELL, I DON'T KNOW, BECAUSE THE F5 DOESN'T TELL ME!"

Actually, the F5 can tell you if you know where to look. The statistics aren't attached to the application's virtual server: they are collated at the associated client-ssl profile. Suppose that a customer has a created a client-ssl profile named 'ssl-exchange-2'. He or she can then query the protocol counters via the following tmsh command.

```
[davidh@murky:Active] ~ # tmsh show ltm profile client-ssl ssl-exchange-2
```

The output will include the protocol counts (excerpted here).

```
-------------------------------------------------------------------------------
Ltm::ClientSSL Profile: ssl-exchange-2
-------------------------------------------------------------------------------
Virtual Server Name                                          N/A

Bytes                                                    Inbound  Outbound
  Encrypted                                                5.8M     14.7M
```

```
  Encrypted                                                 5.8M      14.7M
  Decrypted                                                 1.1M       2.0M

...

Protocol
  SSL Protocol Version 2                                       0
  SSL Protocol Version 3                                      21
  TLS Protocol Version 1.0                                    32
  TLS Protocol Version 1.1                                    54
  TLS Protocol Version 1.2                                   282
  DTLS Protocol Version 1                                      0
```

In order for a customer to know if he can safely disable SSLv3, he has to know how much SSLv3 his site is still processing. If it's a non-trivial amount, then they'll probably want to wait. Google, for example, was behind the POODLE announcement, but they still accept SSLv3.

F5 has some customers who report that up to 15% of their traffic is SSLv3. They aren't willing to trade that 15% for an A grade from SSL labs. Most customers have no idea what their traffic split is.

The **tmsh** command above can give you the counts you need, but just for fun, let's cook up an iRule that will categorize SSL traffic using the **iStats** statistical aggregator doo-dad. The iStats feature is so cool that F5 barely documents it or promotes it in any way.

With iStats we can create customized statistics, and associate those stats with existing F5 configuration objects. So the heart of our iRule will be this little phrase:

```
when CLIENTSSL_HANDSHAKE {
        ISTATS::incr "ltm.virtual [virtual name] c [SSL::cipher version]" 1
    }
```

The code phrase simply creates statistical values named 'SSLv3', 'TLSv1', 'TLSv1_1' and 'TLSv1_2' and associates them with the virtual server (returned by [virtual name]) that the iRule is attached to at runtime.

If we were to attach that iRule snippet to your virtual server named "stdsslvip," then we could actually see the statistics with a normal 'tmsh show' command!

```
[davidh@murky:Active] ~ # tmsh show ltm virtual stdsslvip
```

and the result looks like this:

```
-----------------------------------------------------------------
Ltm::Virtual Server: stdsslvip
-----------------------------------------------------------------
Status
  Availability     : available
  State            : enabled
  Reason           : The virtual server is available
  CMP              : enabled
  CMP Mode         : all-cpus
  Destination      : 192.168.2.189:443

Traffic                             ClientSide  Ephemeral  General
  Bits In                              872.0K          0        -
  Bits Out                               3.7M          0        -
```

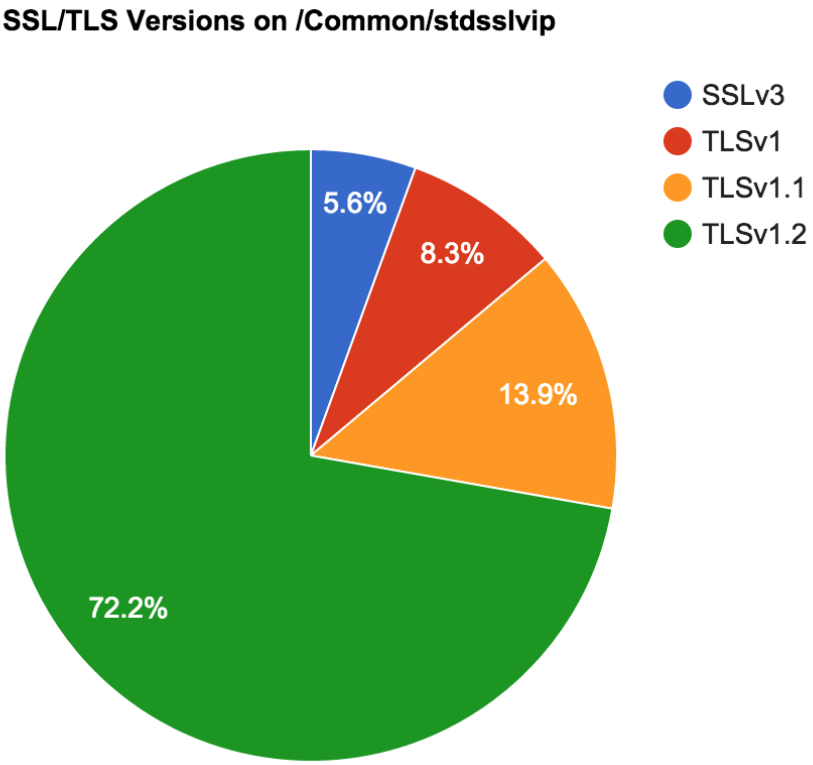
```
  Packets In                              943          0        -
  Packets Out                             871          0        -

User-defined  Value
  SSLv3     21
  TLSv1     32
  TLSv1.1   54
  TLSv1.2  282
```

Binding the statistics directly to the virtual server is pretty neat, but by pulling in the Google Charts javascript widget, we can have the iRule display a cool, interactive graph. We'll trigger the graph by watching for the URL "/sslversions".

In our browser, we enter **https://<stdsslvip>/sslversions**.

And then, voila, we get a pretty page back. This is the kind of page that we can include in our weekly TPS report to our so-called superior.



If we want to query more than one virtual server at at time, we can use the handy-dandy istats dump command like this:

```
[davidh@murky:Active] ~ # istats dump

all facts:

[ ltm.virtual=/Common/stdsslvip ][TLSv1.1] = 54 (2015-09-01 13:52:20)
[ ltm.virtual=/Common/stdsslvip ][SSLv3] = 21 (2015-09-01 13:52:20)
[ ltm.virtual=/Common/stdsslvip ][TLSv1.2] = 282 (2015-09-01 13:52:20)
[ ltm.virtual=/Common/stdsslvip ][TLSv1] = 32 (2015-09-01 13:52:20)
```

By using the iRule, you can tell how much of your traffic is SSLv3. Once you have the breakdown of SSL versions, you can make knowledgeable decision about whether or not to disable SSLv3.

My recommendation is that if even 5% of your traffic is SSLv3, keep it enabled. POODLE was mostly a browser issue anyway. Just be sure that you use a stream cipher like RC4. You can find more information about how configure SSLv3 with RC4 from Jeff Costlow's article: SSLv3 POODLE mitigation recommendations.

And finally, here's a link to the iRule code snippet.

https://devcentral.f5.com/codeshare/categorize-ssl-traffic-by-version-display-as-graph

Use as you see fit, and if you have any modifications send them my way and I'll merge them into the codeshare.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com