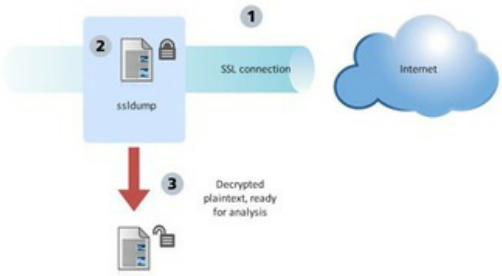
Giving back to the Dev Community: ssldump data decrypt

David Holmes, 2011-14-12

Now with TLS1.2 support, #infosec

In my previous post, I announced that I've traded in my compilers for frequent flier miles and spell chekkers. (ha, joke). That's right; I'm in the marketing department now. But before I go, I wanted to give one last salute to the Development Community that I served in for so long.



There's an open-source tool called **ssldump**, written by the Chairman of the IETF TLS committee himself, Eric Rescorla. The tool is actually quite mature (by which we mean old) and the primary development work was done right after SSL3 was tweaked, formalized, and named TLS over ten years ago. If you look at the changelog, one of the very last changes was submitted by F5 Network's very own Jeffrey Hafey who added VLAN tag support back in 2000. Jeffrey was one of our most brilliant Enterprise Network Engineers at the time; I remember being on the phone with him and I asked what times of day I should call him, because at the time, he was based out of Japan. "Call me anytime" he said. "No, really, when can I call?" I said. "Seriously, anytime, I don't sleep." And I don't think he did.

F5 has included the ssldump utility on the BIG-IP platform since those early days. You can even run it from our TMOS shell command interpreter like so:

```
(tmos) # run util ssldump -i external -s0 -d -k /config/ssl/ssl.key/default.key port 443
```

In the example above, the syntax means "decrypt the SSL traffic coming from the external interface using this key." It's a handy tool to have when debugging HTTPS issues. Also, F5's version of the ssldump utility even decrypts traffic encrypted with your FIPS 140 keys! Don't worry, that's not a security leak, it's a diagnostic feature that only works when you run it on the same device that has the key.

Like many browsers and other SSL tools, **ssldump** doesn't support the newer versions of the TLS protocol (1.1 and 1.2) when decrypting application data.

Until now.

I'm posting a patch to SourceForge that adds TLS1.1 and 1.2 support for decrypting application data. Basic unit testing has been run on it and before you chide me about using magic numbers for my buffer lengths, the patch is following the convention of the existing code around keep the changes as manageable as possible. **BIG-IP Versions 10.2.4 and 11.2.0** should have these fixes. You can download the patch yourself and apply it to your own Ubuntu, Debian, or CentOS release; if you find deficiencies in the patch, just email me and we'll see if we can make it better.

There is no doubt that our competitors will pick up the changes and integrate them into their own tools, but you know what? That's okay. F5 is the market leader in SSL processing and this is just how we roll.

In a future post we'll take a look at why there's suddenly a lot of interest in TLS1.2.

- Troubleshooting TLS problems With ssldump
- Mutations in the TLS Protocol

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