Tunnelblick and openvpn_xorpatch - Tunnelblick

5-7 minutes

On This Page

The openvpn_xorpatch Controversy

A patch to add a "scramble" option to OpenVPN was proposed in April, 2013. The option can be useful to avoid having OpenVPN traffic detected by monitoring or censoring mechanisms such as the Great Firewall of China. The option "scrambles" each buffer of traffic before it is sent between the OpenVPN client and server.

However, the patch is controversial: it was not accepted as an addition to OpenVPN by the OpenVPN developers. There was a long discussion of the patch on the OpenVPN Community Support Forum. The discussion has been removed, but the last post was:

> "We (OpenVPN developers) do not encourage people building their own versions of OpenVPN changing the wire-protocol like this, without the patch being through a proper patch review and having evaluated possible security risks related to such a change.
>
> "And we especially discourage using such an approach when there exists a far better solution, used by the TOR community. It is called obfsproxy and can be used together with OpenVPN without needing any re-compilation of OpenVPN.
>
> "For more information, have a look at these URLs
> OpenVPN Traffic Obfuscation
> Tor obfsproxy"
>
> "To avoid confusing users further going for a possibly insecure setup , this thread will be locked now."

In December 2016, further discussion took place on the OpenVPN users mailing list. OpenVPN developers again explained why they do not want to include the patch in OpenVPN and discussed alternatives. See (https://sourceforge.net/p/openvpn/mailman/openvpn-users/thread/DFBD5589-71CB-41CD-B7A7-F2A540380E33%40haloprivacy.com/#msg35560747.

Tunnelblick's View

Regardless of the OpenVPN developers decision not to include the patch in OpenVPN, the patch is attractive because it is so easy to implement: simply apply the patch to both the OpenVPN server and the OpenVPN client and add a single, identical option to the configuration files for each. Using obfsproxy is more complicated because it involves running another, separate program on both the server and the client.

Because the patch is so easy to implement, the patch is included in all versions of OpenVPN that are included in Tunnelblick as of build 4420.

Critical Warning

The original post proposing the patch claims that using the patch is sufficient to secure communications and that no other encryption is necessary:

> "With this obfuscate option, I think that it is ok to use "cipher none", because working out the method used would take a lot of cryptoanalysis. The obfuscate option is also much easier on the CPU than any cipher options This is incase you are using ddwrt or openwrt or have a low speed cpu."

Do not take this advice! The obfuscation provided by this patch appears to be extremely rudimentary. Beware of cryptographic advice from amateur cryptographers!

Large organizations have the ability and power to "unscramble" traffic and detect it as OpenVPN traffic, and the obfuscation provided by this patch is so rudimentary that relatively simple cryptanalysis will probably be able to unscramble the content, too.

Tunnelblick Modifications to the Patch

As the OpenVPN developers point out, the patch has never been through a thorough review for security, coding, etc. However, a Tunnelblick developer has reviewed the patch, found some problems, and modified it in Tunnelblick to resolve those problems. The problems that were found and fixed involved insufficient parameter validation, null pointer dereferences, division by zero errors, and a buffer overflow. Some defensive programming was also added to the modified version of the patch to increase its robustness.

I invite anyone/everyone to review the patch and report any problems, either to the Tunnelblick Discussion Group or to the developers. Details of the patch are below.

Scramble Option Syntax

Note: The "scramble" option and parameters in the server and client configuration files must match.

scramble *xor_string*
scramble xormask *xor_string*
These options XOR the bytes in each buffer with *xor_string*.

scramble reverse
The "reverse" option reverses order of the bytes in each buffer (except that the first byte is unchanged). So "abcde" becomes "aedcb".

scramble xorptrpos
The "xorptrpos" option XORs each byte of the buffer of traffic with the position in the buffer.

scramble obfuscate *password*
The "obfuscate" option performs several of the above steps, using *password* as the *xor_string* in one of the steps.

The Patch as Modified for Use in Tunnelblick

Tunnelblick's build process expands OpenVPN, applies patches, and then builds from the patched source code.

In recent versions of Tunnelblick, the patch has been broken into five separate .diff files, with each .diff modifying a single file in the OpenVPN source code. (This is done to make it easier to modify the patch when the underlying OpenVPN source code is changed.)

Files with patches for each particular version of OpenVPN are located in the Tunnelblick source code in a "patches" folder specific to that version of OpenVPN. The path to patches for OpenVPN version X.Y.Z would be

```
.../third_party/sources/openvpn/X.Y.Z/patches
```