1 Summary

The authors expose vulnerabilities related to OpenVPN, the most popular protocol for commercial VPN services. Specifically, they show how despite OpenVPN's implementation of widely applied obfuscation techniques, usage can be *reliably* detected and blocked at-scale by "network-based adversaries." Although the authors propose some short-term mitigation strategies, they advise VPN providers to improve their obfuscation approaches in the long term.

2 Strengths of the paper

1. It is a noble endeavor undertaken by the authors to find vulnerabilities within commercial VPN services to protect and preserve the unknowing users' privacy. Rather than just pointing these vulnerabilities out, the authors also suggest some short-term mitigation strategies such as spatially separating vanilla and obfuscated VPN instances, making VPN providers switch from static to random padding for their obfuscated services, and modifying servers' response(s) to failed handshake attempts.
2. This work obviously has potential to lend itself to questionable ethical, privacy and responsibility considerations. But the authors do a fine job of mitigating any such concerns by outlining how the framework does not compromise any such aspect of *Merit*'s network in §5.
3. The *Filter* implementation in Zeek (open-source network monitoring tool) and the *Prober* implementation in Nim as a means to perform opcode, ACK-based fingerprinting (*Filter*), and filter results to lower false positives, is a relatively simple evaluation process.

3 Weakness of the paper

I know this wasn't the goal of the paper, but it felt wanting about the long-term defenses against the censoring parties employed by the circumvention tools. Sure, urging VPN providers to adopt next-generation obfuscation techniques like Pluggable Transports and to increase transparency about obfuscation techniques is good, but discussion about the limitations of this approach may have yielded more well-roundedness.

4 Future work opportunities

Have commercial VPN services adopted the approaches suggested by this paper yet? If so, to what extent? If not, what prevents them from doing so? Perhaps a literature review on the state of implementation within the aforementioned services w.r.t this paper's suggestions is a worthy use of some authors' time...

Reference

D. Xue et al., "OpenVPN is Open to VPN Fingerprinting," presented at the 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 483–500.