Short Research Proposal for MPhil ACS

C Shi

For postgraduate research in the fields of cryptography and network security, I am particularly interested in obfuscating encrypted network traffic against protocol classification [1] and active probing [2] by deep packet inspection (DPI) systems, which are utilised by both commercial firewalls and more controversially, state censors to block encrypted connections. In general, two categories of techniques exist to achieve obfuscation of the encrypted traffic: pseudo-random transformation and fronting of other "legitimate" protocols.

The *ScrambleSuit* Protocol by Winter *et al.* [3] implements Uniform Diffie-Hellman with pre-shared key authentication to prevent active probing and applies pseudo-random polymorphism to diminish the effectiveness of traffic analysis. However, it leaves open the lack of concealment of the "burstiness" of traffic. *Format-Transforming Encryption* (FTE) designed by Dyler *et al.* [4] intentionally misleads DPI by transforming the format of ciphertext, with better performance compared to *ScrambleSuit*, but lacks protection against active probing. Furthermore, entropy-based attacks by Wang *et al.* [5, Sec. 5] have been shown to be effective against these obfuscation protocols at relatively low computational costs and misclassification rates (around 4%).

The flaws in *ScrambleSuit* and FTE that render them vulnerable to entropy-based attacks are mainly related to their initial phases of connection, during which a secure connection is established over an insecure channel. Messages exchanged during this phase are distinguishable by higher entropy due to their lack of similarities to a "legitimate" protocol, whose initial messages are often distinctive and unencrypted [5, p. 58]. Therefore, the deliberate designs for pseudo-randomness (often requiring out-of-band key exchange [6, Fig. 4], thus reducing usability) may have caused the opposite effect to obfuscation: their traffic could be easily detected through identifying initial messages.

This vulnerability is largely resolved by fronting techniques such as those deployed by Meek [7], for which entropy-based attacks by Wang *et al.* [5, Sec. 6] are not as effective. Meek mimics standard TLS connections [6, Sec. 3], which carries a very significant overhead [7, Fig. 3] but makes it difficult for both passive analysis and active probing to achieve their purposes with precision. A TLS-style connection also allows more convenient in-band key exchanges to take place [6, Fig. 4].

This sets out a trade-off: fronting other protocols is an effective protection against entropy-based attacks, but the high overhead incurred could be detrimental to the connection quality, not to mention the quality of fronting itself may affect the protocol's ability to evade detection [6, p. 2]. Therefore, potential areas of work could seek to balance both worlds: fronting techniques could be adapted to make initial phases of pseudo-random transformation protocols less distinguishable; and the performance of existing protocols base on fronting can be improved by adapting more efficient methods currently putting into use by the fronted protocols. A prime example of the latter is the potential adoption of 1-RTT handshakes in TLS 1.3 [8]. I intend to explore the feasibilities of both possible areas of work.

References

[1] M. Crotti *et al.*, "Traffic classification through simple statistical fingerprinting," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 1, pp. 5–16, 2007.

[2] R. Ensafi *et al.*, "Examining how the great firewall discovers hidden circumvention servers," in *Proceedings of the 2015 ACM Conference on Internet Measurement Conference*, pp. 445–458, ACM, 2015.

[3] P. Winter *et al.*, "Scramblesuit: A polymorphic network protocol to circumvent censorship," in *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, pp. 213–224, ACM, 2013.

[4] K. P. Dyer *et al.*, "Protocol misidentification made easy with format-transforming encryption," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 61–72, ACM, 2013.

[5] L. Wang *et al.*, "Seeing through network-protocol obfuscation," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 57–69, ACM, 2015.

[6] L. Dixon *et al.*, "Network traffic obfuscation and automated internet censorship," *IEEE Security & Privacy*, vol. 14, no. 6, pp. 43–53, 2016.

[7] D. Fifield *et al.*, "Blocking-resistant communication through domain fronting," *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 46–64, 2015.

[8] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3.* Network Working Group, IETF, draft 19 ed.