# Project Description for Degree Projects Department of Computer Science

|  |  |  |
| --- | --- | --- |
| Student: | Songho Lee | [sl222xk@student.lnu.se](mailto:sl222xk@student.lnu.se) |
| Supervisor: | Ola Flygt (communications are ongoing) | |
| Draft title: | Evaluation of DNS-over-HTTPS as a supplementary solution for bypassing web filters | |

# Background

Large scale monitoring is a threat towards users of the Internet. Information collected in such action could lead to a breach of users’ privacy or could become aids for launching an active form of attacks, such as masquerade and denial of service.

The ecosystem of the Internet has changed in recent decennial: few Internet firms such as Google, Facebook, and Amazon dominate their relevant markets nearly as monopoly [1]; It has become more common to have web services deployed in cloud environments [2]. These phenomena led the endpoints of Internet traffics to be more centralised than ever. Also, another notable change of the Internet is that adoption of HTTPS on the web has increased significantly [3, 4].

The centralised Internet brings more challenges to the traditional form of traffic monitoring. Such as, following by source and destination of IP traffics may not be applicable for many cases anymore, as more servers are co-hosted in diverse IaaS providers.

# Problem formulation

Wide deployment of encryption protocols, such as HTTPS, brought challenges in payload-based traffic classification [5]. Despite the achievement of securing communication channels, there is room for legacy web-filtering to work, such as Domain Name System (DNS) filtering. Currently, almost all DNS traffic is sent in clear text over UDP protocol, which makes DNS queries vulnerable to being hijacked and filter users traffics.

Monitoring traffics based on domain queries, however, could be circumvented by securing clients’ DNS queries, and one of the methods to secure DNS queries is to use DNS-over-HTTPS (RFC 8484) or DNS-over-TLS (RFC 8310).

# Expected Result

The project aims to apply one of DNS encryption protocols as described above as a method of securing DNS queries, and test whether it helps bypassing firewall or other traffic monitoring solutions’ web filtering.

The ambition is to demonstrate that applying DNS encryption together with currently used HTTPS overcomes web filters. However, in case of not managing it, it is anticipated to analyse which other weakness could be identified.

Works Cited

|  |  |
| --- | --- |
| [1] | J. Haucap and U. Heimeshoff, “Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization?,” *International Economics and Economic Policy,* vol. 11, no. 1-2, pp. 49-61, 2014. |
| [2] | Statista, “Current and planned usage of public cloud platform services running applications worldwide in 2018,” Statista, February 2018. [Online]. Available: https://www.statista.com/statistics/511467/worldwide-survey-public-coud-services-running-application/. [Accessed 27 January 2019]. |
| [3] | A. P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel and P. Tabriz, “Measuring HTTPS adoption on the web,” *26th USENIX Security Symposium,* pp. 1323-1338, 2017. |
| [4] | W. M. Shbair, T. Cholez, A. Goichot and I. Chrisment, “Efficiently bypassing SNI-based HTTPS filtering,” in *IFIP/IEEE International Symposium on Integrated Network Management (IM)*, Ottawa, 2015. |
| [5] | Y. Xue, D. Wang and L. Zhang, “Traffic classification: Issues and challenges,” in *Computing, Networking and Communications (ICNC), 2013 International Conference on*, San Diego, CA, 2013. |