What can (normal) users do to you protect your privacy online? Consider private browsing mode, VPNs, Tor, anti-tracking add-ons? What are relevant use cases and what risks are involved in the various approaches?

To protect ones privacy, users have a multitude of methods available which complement each other to achieve the common goal.

Nowadays, most modern browsers ships with a private browsing mode. However, it only works for your local machine. *Firefox* states that visited pages, cookies, searches and temporary files are not saved, while bookmarks and downloads still are saved to your PC.(R) This helps users to protect their privacy from a local attack vector, for example when using shared computers.

Another feature that modern browser provide to their users, either direct or indirect through add-ons, is anti-tracking protection. Users can get tracked by a variety of methods. *Facebook Inc.* for example is able to collect user data on every website where their frames for liking or sharing are embedded. (More research) Anti-tracking protection tries to recognize said elements on a website and prohibit them from loading. The drawback is, that sometimes some features of a website could stop working.

There is a large number of publications on security issues of the Domain Name System (DNS), most of them are concerned with DNSSEC [1]. Privacy issues have only recently been found to be interesting [2]. An overview of security and privacy issues in the DNS is presented by Conrad [6].

The range query technique protects the privacy of users who submit DNS queries to a DNS resolver. The basic range query scheme was introduced by Zhao et al. in [10]; there is also an improved version [11] inspired by private information retrieval [5]. Although the authors suggest their schemes especially for web surfing applications, they fail to demonstrate their practicability using empirical results.

Castillo-Perez and Garcia-Alfaro propose a variation of the original range query scheme [10] using multiple DNS resolvers in parallel [3,4]. They evaluate its performance for ENUM and ONS, two protocols that store data within the DNS infrastructure. Finally, Lu and Tsudik propose PPDNS [8], a privacy-preserving resolution service that relies on CoDoNs [9], a next-generation DNS system based on distributed hash tables and a peer-to-peer infrastructure, which has not been widely adopted so far.

The aforementioned publications study the security of range queries for singular queries issued independently from each other. In contrast, [7] observes that consecutively issued queries that are dependent on each other have implications for security. They describe a timing attack that allows an adversary to determine the actually desired website and show that consecutive queries have to be serialized in order to prevent the attack.

Note: The LaTeX source of this document contains further remarks and hints.

References

1. Arends, R., Austein, R., Larson, M., Massey, D., Rose, S.: DNS Security Introduction and Requirements. RFC 4033 (Mar 2005)
2. Bortzmeyer, S.: DNS Privacy Considerations. RFC 7626 (2015)
3. Castillo-Perez, S., García-Alfaro, J.: Anonymous Resolution of DNS Queries. In: On the Move to Meaningful Internet Systems. pp. 987–1000. Springer, LNCS 5332 (2008)
4. Castillo-Perez, S., García-Alfaro, J.: Evaluation of Two Privacy–Preserving Protocols for the DNS. In: International Conference on Information Technology: New Generations (ITNG 2009). pp. 411–416. IEEE (2009)
5. Chor, B., Goldreich, O., Kushilevitz, E., Sudan, M.: Private Information Retrieval. In: Symposium on Foundations of Computer Science. pp. 41–50. IEEE (1995)
6. Conrad, D.: Towards Improving DNS Security, Stability, and Resiliency (2012), http://internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf
7. Federrath, H., Fuchs, K.P., Herrmann, D., Piosecny, C.: Privacy-Preserving DNS: Analysis of Broadcast, Range Queries and Mix-Based Protection Methods. In: European Symposium on Research in Computer Security (ESORICS 2011). pp. 665–683. Springer, LNCS 6879 (2011)
8. Lu, Y., Tsudik, G.: Towards Plugging Privacy Leaks in the Domain Name System. In: International Conference on Peer-to-Peer Computing. pp. 1–10. IEEE (2010)
9. Ramasubramanian, V., Sirer, E.: The Design and Implementation of a Next Generation Name Service for the Internet. In: SIGCOMM. pp. 331–342. ACM (2004)
10. Zhao, F., Hori, Y., Sakurai, K.: Analysis of Privacy Disclosure in DNS Query. In: International Conference on Multimedia and Ubiquitous Engineering. pp. 952–957. IEEE (2007)
11. Zhao, F., Hori, Y., Sakurai, K.: Two–Servers PIR Based DNS Query Scheme with Privacy–Preserving. In: International Conference on Intelligent Pervasive Computing. pp. 299–302. IEEE (2007)