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.

Aggarwal et. al. state that every modern browser ships with a private browsing mode [1]. In private browsing mode visited pages, cookies, searches and temporary files are not saved to the local disk, while bookmarks and downloads still are. This helps users to protect their privacy from a local attack vector. However, it is important to note that it only protects if the attacker only has access to the pc after the user exits private browsing. Otherwise the local machine could already be compromised by the attacker, f.e. by using a keylogger.

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 [2]. Privacy issues have only recently been found to be interesting [3]. An overview of security and privacy issues in the DNS is presented by Conrad [7].

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 [11]; there is also an improved version [12] inspired by private information retrieval [6]. 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 [11] using multiple DNS resolvers in parallel [4,5]. They evaluate its performance for ENUM and ONS, two protocols that store data within the DNS infrastructure. Finally, Lu and Tsudik propose PPDNS [9], a privacy-preserving resolution service that relies on CoDoNs [10], 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, [8] 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. Aggarwal, G., Bursztein, E., Jackson, C., Boneh, D.: An analysis of private browsing modes in modern browsers. In: Proceedings of the 19th USENIX Conference on Security. pp. 6–6. USENIX Security'10, USENIX Association, Berkeley, CA, USA (2010), http://dl.acm.org/citation.cfm?id=1929820.1929828
2. Arends, R., Austein, R., Larson, M., Massey, D., Rose, S.: DNS Security Introduction and Requirements. RFC 4033 (Mar 2005)
3. Bortzmeyer, S.: DNS Privacy Considerations. RFC 7626 (2015)
4. 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)
5. 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)
6. Chor, B., Goldreich, O., Kushilevitz, E., Sudan, M.: Private Information Retrieval. In: Symposium on Foundations of Computer Science. pp. 41–50. IEEE (1995)
7. Conrad, D.: Towards Improving DNS Security, Stability, and Resiliency (2012), http://internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf
8. 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)
9. 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)
10. Ramasubramanian, V., Sirer, E.: The Design and Implementation of a Next Generation Name Service for the Internet. In: SIGCOMM. pp. 331–342. ACM (2004)
11. 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)
12. 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)