Protect DNS from Distributed Denial of Service Attacks

This is an external assignment to be carried on in collaboration with SURFnet, Utrecht (http://www.surfnet.nl).

The global DNS infrastructure has a long of history of being abused for (Distributed) Denial of Service (DDoS) attacks. DNS reflection and amplification attacks have the potential to paralyze entire institutions or networks. Although disruptive, these attacks took place on a relatively modest scale. In recent times, however, we see a worrying escalation in the application of this kind of attack. We see (attempts of) abuse of our DNS servers to facilitate these kinds of attacks. SURFnet and its connected institutions are also victims.

The goal of the thesis work will be to investigate whether, and if so how, it is possible to detect these kinds of attacks based on the characteristics of incoming DNS queries. Not only the query itself is of interest but also aspects like the query rate, parameters used in subsequent queries and the datagrams containing the queries and other protocol parameters in different network layers (DNS(SEC), UDP, TCP, IP, etc.).

Besides detection of (potential) attack attempts the research should also address how such attempts can (or cannot) be automatically blocked without hindering legitimate use of DNS(SEC).

For more information about this assignment, please contact:

- Aiko Pras: a.pras@utwente.nl
- Anna Sperotto: a.sperotto@utwente.nl
- Roland van Rijswijk – Deij: Roland.vanRijswijk@surfnet.nl
- Xander Jansen: Xander.Jansen@surfnet.nl