Ph.D. Student Vacancy on “DDoS mitigation with IP anycast” at the University of Twente

We are looking for an energetic PhD student holding an MSc degree in Computer Science/Engineering. The candidate should have a strong computer networking background, routing, and willingness to work with real-world deployments.

Research Project Description

Distributed Denial-of-Service (DDoS) attacks are a continued and growing challenge for Internet services. Denial-of-Service aims to overwhelm network services using a large amount of traffic affecting the availability of the services. Assorted mechanism of defense has been studied to protect systems from such attacks, however, in behalf of complexity and magnitude of such attacks defenses should be improved. In particular, source-address spoofing, protocols amplification attacks and botnet of thousands of machines widespread are factors that boost today’s Distributed Denial-of-Service attacks. In the remarkable attack of Dyn [1], a botnet composed by multi-thousand-nodes, mainly Internet-of-Things (IoT) devices, has used to launch DDoS attack affecting providers all over the world.

The Internet infrastructure, such as DNS service is also affected by large-scale DDoS attacks [2]. Since spoof and amplification attacks prevention does not eliminate the threat of large botnet attacks and filtering is not effective against sophisticated attacks, is necessary to investigate a cost-effective method to reach DDoS-tolerant capacities, such as anycast [3]. Anycast allows spreading a service over multiples sites enabling to handle the traffic based on the site capabilities. Although anycast is widely used in DNS and CDNs today, existing tools to manage anycast are very limited. Furthermore, there are no tools to assist in the process of reconfiguring the anycast network when a DDoS attack is detected.

The Ph.D. candidate in this position will work on a joint NL/US research project which the goal is to counter the IoT DDoS threat by making anycast-based capacity effective for global DNS system.

For application and further information, please contact:

Dr. João Ceron: j.m.ceron@utwente.nl

References:

[1] https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

[2] http://www.isi.edu/%7ejohnh/PAPERS/Moura16b.pdf

[3] https://conferences.sigcomm.org/imc/2017/.../imc17-final46.pdf