MADDVIPR: Mapping DNS DDoS Vulnerabilities to Improve Protection and Prevention

Dr. Anna Sperotto & Dr. Kimberly Claffy

Het Domain Name System (DNS) vervult een cruciale taak op het internet: het vertalen van voor mensen leesbare namen in voor machines leesbare IP adressen. Daarmee ondersteunt DNS vrijwel alle internetdiensten, waaronder mediadiensten en veiligheidsvoorzieningen. Omdat het internet zo afhankelijk is van DNS, zijn Distributed Denial-of-Service (DDoS)-aanvallen gericht op DNS zeer schadelijk. Het doel van het MADDVIPR project is het systematisch in kaart brengen van: 1) kwetsbaarheden in de inrichting van DNS, en 2) aanvalsbronnen, aanvallers en doelwitten van DDoS-aanvallen op het DNS. We brengen deze twee delen van het onderzoek vervolgens bij elkaar om een eenduidig beeld te krijgen van het dreigingslandschap richting DNS. Hiermee kunnen we a) inzicht krijgen in lopende aanvallen tegen DNS, b) inzicht krijgen in kwetsbaarheden en met welke prioriteit deze door DNS operators moeten worden opgelost en c) operators richtlijnen geven om zich tegen toekomstige aanvallen op DNS te wapenen. Dit project brengt unieke databronnen uit eerder onderzoek samen: het OpenINTEL project, wat dagelijks 60% van het wereldwijde DNS bemeet, en internetbrede metingen van CAIDA, waaronder de Network Telescope, een grootschalig zogenaamd \darknet" waarmee op basis van achtergrondruis DDoS aanvallen kunnen worden waargenomen. De schaal van deze datasets is in de orde van tera- tot petabytes per jaar. Aan de ene kant biedt dit een unieke kans om een groot deel van het internet te dekken in de analyse, aan de andere kant zijn er grote uitdagingen te overwinnen in het vinden en combineren van de juiste informatie.