MINIONS: MitigatINg IOt-based DDoS attacks via DNS

Dr. ing. C. Hernandez Ganan & Dr. D. McCoy

Slechte beveiliging van Internet-of-Things-apparatuur (IoT) vormt een groot veiligheidsrisico voor kritieke internetinfrastructuren en kan tot significante schade leiden. Ter illustratie, Dyn, een grote Domain Name System (DNS) provider, werd getroffen door een grote Distributed Denial-of-Service (DDoS) aanval die gebruik maakte van gehackte IoT apparaten. Als gevolg hiervan werden grote internetdiensten als Airbnb, PayPal, CNN, The New York Times en Twitter deels verstoord. In dit project focussen we op het ontwerpen, bouwen en evalueren van praktische technieken en instrumenten om de bedreiging van DDoS-aanvallen vanaf IoT-apparatuur terug te dringen. De eerste verbetering die we zullen realiseren is het MINION's instrument voor in-home netwerken. Dit instrument maakt gebruik van DNS om geïnfecteerd IoT apparaten te detecteren. De resultaten van deze vorm van detectie zal gebruikt worden voor zowel DNS-gebaseerde filtering en het opschonen van geïnfecteerde IoT-apparatuur. Daarnaast zullen op basis van dit voorstel geautomatiseerde instrumenten gebouwd worden om inzicht in de structuur te krijgen van criminele DDoS-for-hire diensten. Deze kennis zal gebruikt worden om de geldstromen tussen klanten en services te verstoren en andere mogelijk interventies te ontwerpen. Onze technieken en instrumenten zullen we overbrengen naar commerciële anti-DDoS-diensten, online betalingsverleners en threat intelligence bedrijven. Zij kunnen onze praktische mitigatiestrategieën implementeren en daarmee het risico op IoT-gebaseerde DDoS-aanvallen verminderen.