BASIC PROGRAMMATIC DATA

Performer: CAIDA, University of California San Diego (UCSD)
Project: DHS S&T cooperative agreement FA8750-19-2-0004
    Mapping Domain DNS DDoS Vulnerabilities to Improve Protection and Prevention
Period of Performance (base): November 1, 2018 – October 31, 2022
Total Award Value: $250,000

PROJECT PROGRESS

Progress Against Planned Objectives:

UCSD assisted UT in performing an analysis of State of the Art of DNS vulnerabilities and DNS DDoS attacks.
UCSD helped writing a poster proposal that has been accepted for presentation at ICT.OPEN 2019 Conference.
UCSD gave a talk on MADDVIPR and presented a poster at the DHS Cybersecurity and Innovation Showcase.
Monthly conference calls between UT and CAIDA are taking place to discuss the project progress.

Technical Accomplishments this Period: none

Improvements to Prototypes this Period: none

Significant Changes to Technical Approach to Date: none

Deliverables:
- Y1:M3 - Background research on DNS vulnerabilities

Technology Transition and Transfer this Period: none

Publications this Period:
- MADDVIPR Poster accepted at ICT.OPEN 2019 Conference.

Meetings and Presentations this Period: none

Issues or Concerns: none

PROJECT PLANS

Planned Activities for Year I:
- UCSD will provide feedback and help in investigating the state of the art of DNS DDoS vulnerabilities and misconfiguration.
- UCSD will provide feedback to the Ph. D. student (U. Twente) on his background research on DNS vulnerabilities, and on characterizing existing single points of failure in current DNS setups.

Specific Objectives for Next Period:

UCSD will assist Twente with investigating the parent/child delegation TTL and NS mismatches, the impact on the resilience against DDoS attacks and DNS hijacking, and possible solution to the problem.