Technical Quarterly Report – Oct 2019 - Dec 2019

BASIC PROGRAMMATIC DATA

Performer: University of Twente
Project: 628.001.031(NWO)
Mapping DNS DDoS Vulnerabilities to Improve Protection and Prevention
Period of Performance (base): December 1, 2018 – November 31, 2022

PROJECT PROGRESS

Progress Against Planned Objectives:

UT and CAIDA have investigated the parent/child delegation TTL and NS mismatches by identifying the spread of the phenomenon, the resolvers behavior and possible solutions to the problem writing a paper under review to PAM2020.
UT has expanded the investigation on the orphan DNS records problem in collaboration with CAIDA and UCSD members on investigating dangling resources in the DNS.
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: Identify DNS misconfigurations and suboptimal configurations

Technology Transition and Transfer this Period: none

Publications in this Period:

- The Forgotten Side of DNS: Orphan and Abandoned Records (Work in progress)
- When parents and children disagree: Diving into DNS delegation inconsistency (Under review@PAM2020)

Meetings and Presentations this Period: NWO-DHS PI Meeting, 24 Oct 2019

Issues or Concerns: none

PROJECT PLANS

Planned Activities for Year 2:

- UT and CAIDA will study the network layer architecture of the DNS, in order to identify SPoF and aggregation points in the global DNS infrastructure.
- Using the data provided by OpenINTEL and combining it with other sources UT will identify possible weak points and future attacks.

Specific Objectives for Next Period:
UT will continue the work on orphan records and expand it in collaboration with UCSD
UT & CAIDA will start to work on child-child inconsistency problem and infrastructural SPoF detection