2019 S&T Cybersecurity and Innovation Showcase

Solutions Now I Innovations for the Future

Homeland Security
Science and Technology

MADDVIPR: Mapping DNS DDoS Vulnerabilities to Improve Protection and Prevention

Alberto Dainotti | CAIDA, UC San Diego

March 19, 2019

NWO Netherlands Organisation for Scientific Research

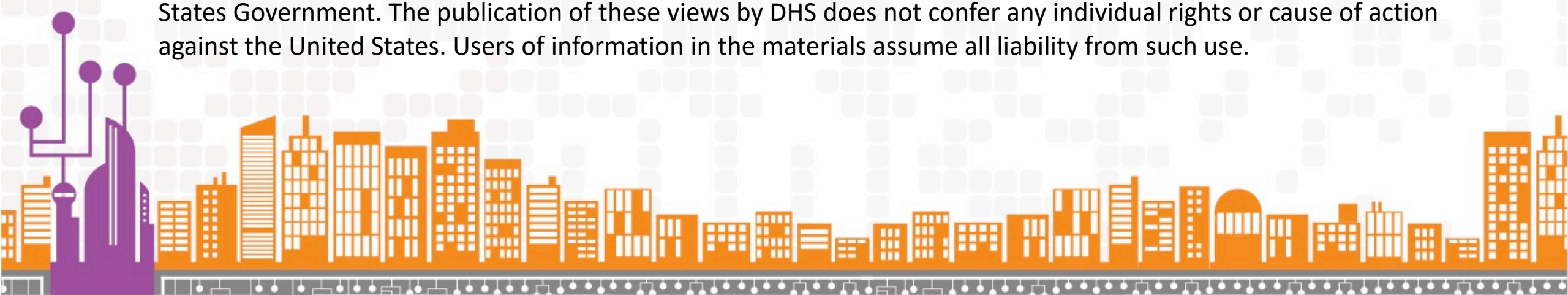
Homeland Security Science and Technology

Funded Contract Information
This material is based on research sponsored by the Department of Homeland Security, Science and Technology Directorate via contract number FA8750-19-2-0004.

No Endorsement Notification
Any reference to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the Department of Homeland Security or the United States Government.

Hyperlinked Web sites do not constitute endorsement by DHS of the Web site or the information, products, or services contained therein. DHS does not exercise any editorial control over materials on this website or the information on non-DHS Web sites.

Disclaimer Notification
The views, opinions, findings, conclusions, or recommendations expressed in this presentation are those of the authors and do not necessarily reflect the official policy or position of the Department of Homeland Security (DHS) or the United States Government. The publication of these views by DHS does not confer any individual rights or cause of action against the United States. Users of information in the materials assume all liability from such use.



Team Profile

- PI: Dr. KC Claffy – Director
- CoPI: Dr. Alberto Dainotti – Research Scientist
- CAIDA – Center for Applied Internet Data Analysis
  University of California, San Diego

- Collaborating PIs: Dr. Anna Sperotto; Dr. Roland Rijswijk-deij
- University of Twente, NL

UNIVERSITY OF TWENTE.

Customer Need

- Protect the DNS from DDoS attacks
  - ***"If you can stop the DNS, you effectively stop most Internet communication"***

- Understanding of the DDoS ecosystem w.r.t. DNS + Systematic analysis of the resilience of the DNS against DDoS
- Tools that generate actionable intelligence to protect the DNS against DDoS attacks

- Customers: Operators and security experts that can benefit from actionable information about the DNS resilience to DDoS attacks.

Approach - Overview

1. Identify DNS single points of failure (SPoF) and vulnerabilities

   To predict how the DNS will be the target of future attacks

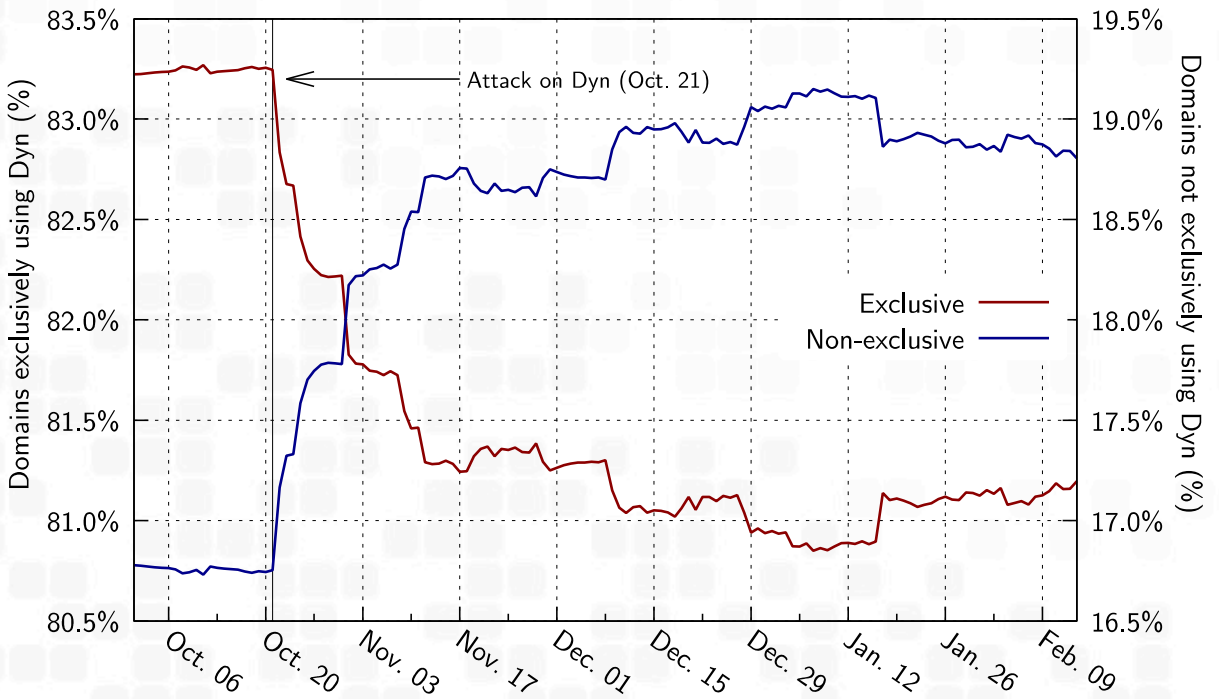
2. Analyze the DNS DDoS ecosystem

   To gain a comprehensive overview of current DDoS attacks against the DNS (attackers, attacks, and targets)

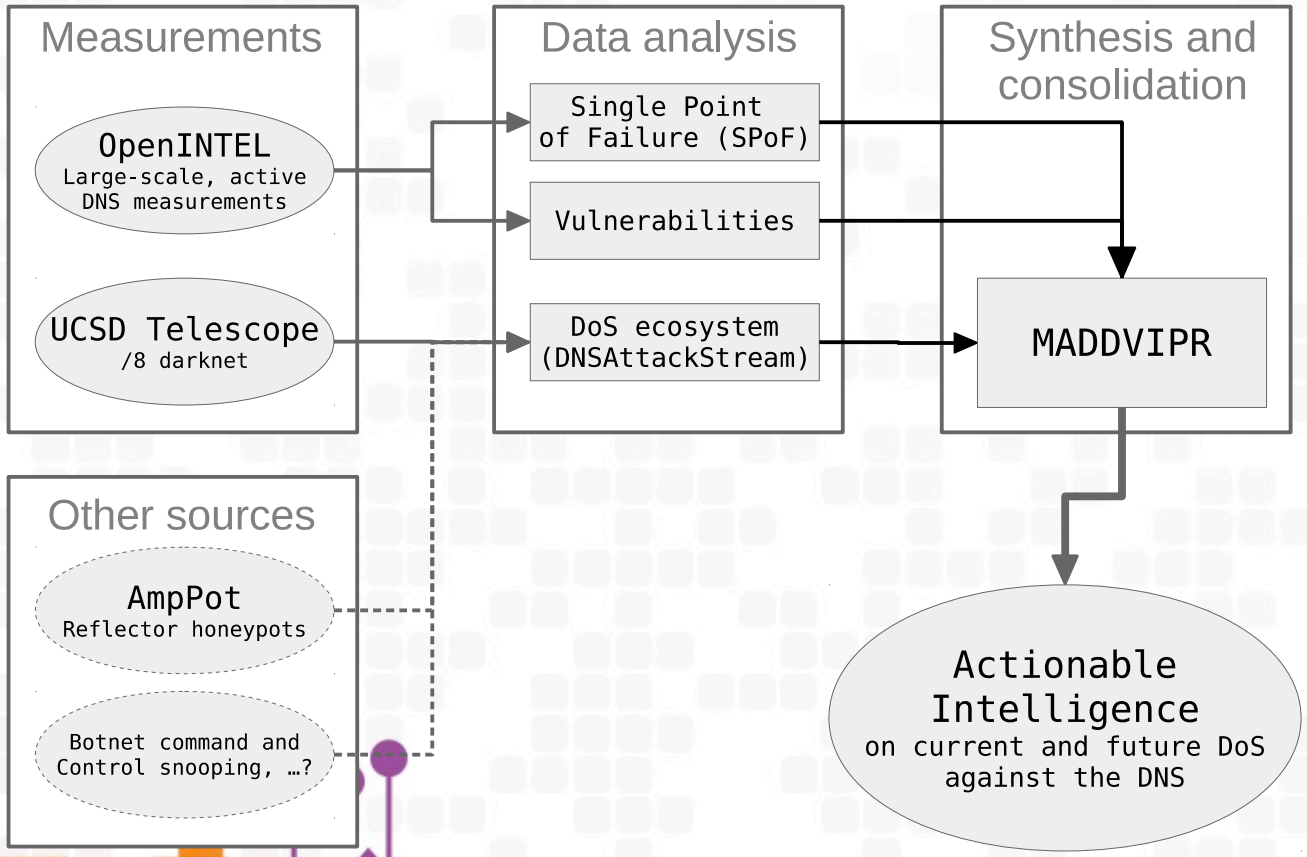
3. Synthesize results of (1) and (2) into a unified view to produce actionable information (for operators and security experts) to improve DNS resilience

Approach - Measurements

- Measurement based approach.
  Key datasets:
  - OpenINTEL project – daily active measurements of >60% of the DNS namespace *(Feb. 2015 – ongoing)*
  - UCSD Network Telescope – inference of DoS attack activity *(Jan 2010 – ongoing)*
- Auxiliary datasets: AmpPot reflection honeypot (University of Saarland), Botnet C&C, …



Approach - Architecture



Benefits

- A rigorous characterization of the DNS DDoS ecosystem and of the DNS vulnerability and misconfiguration
- Operators and security experts: access to **actionable information** in form of e.g. SPoF and misconfiguration blacklists, to improve the resilience and management of their DNS solutions

Competition/Alternatives

- Active DNS measurements
  - Other DNS measurements, e.g. netray.io (RWTH Aachen) and activednsproject.org (GeorgiaTech), exist.
    - In comparisons, OpenINTEL has more comprehensive coverage (65% of the namespace) and has been collecting data the longest (4 years)
  - Alternative: passive DNS measurements; they provide a partial view

- DoS attacks
  - UCSD-NT: unique and comprehensive global view on randomly-spoofed DoS attacks
  - Others provide information about other types of DoS attacks or partial information

Potential Transition Activities

- Open software – whenever suitable, tools will be released as open source
- Open data – a privacy-preserving form of the collected dataset will be made available to researchers
  - CAIDA's 20 years experience in providing curated Internet data
  - OpenINTEL has been awarded the 2018 Netherlands Data Prize for its commitment to making research data available.
- Interaction with operational and standardization bodies (DNS-OARC, IETF/IRTF, ICANN, NANOG, RIPE)

Contact Info

KC Claffy, Alberto Dainotti
CAIDA, University of California San Diego
kc@caida.org, alberto@caida.org
www.caida.org
@caidaorg

2019 S&T Cybersecurity and Innovation Showcase

Solutions Now I Innovations for the Future

Homeland Security
Science and Technology