2019 S&T Cybersecurity and Innovation Showcase

Solutions Now I Innovations for the Future

Homeland Security
Science and Technology

Planning for Anycast as Anti-DDoS (PAADDoS)

John Heidemann | University of Southern California, ISI
Aiko Pras | University of Twente, Computer Science Dept.

March 19, 2019

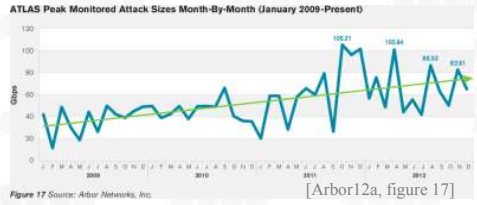
Funded Contract Information
This material is based on research sponsored by the Department of Homeland Security, Science and Technology Directorate via contract number FA87501920003 .

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.

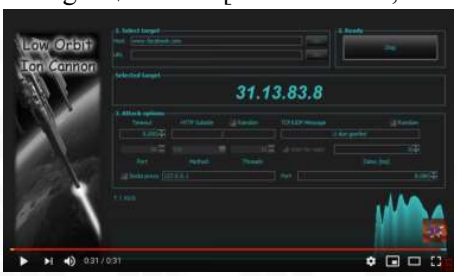
Distributed Denial-of-Service (DDoS) is Bad... and Getting Worse

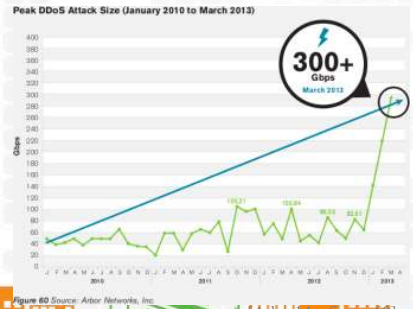


[Arbor12a, figure 17]

big
2012 innovation:
automated botnets
for extortion

cheap: booters offer DDoS-as-a-service
starting at $1/attack [Santanna et al, 2015]





[Arbor14a, figure 60]

bigger
2013 innovation:
DNS amplification

biggest (so far, as of Feb. 2018)
2016: 620 Gb/s KrebsOnSecurity.com
2018: 1.3Tb/s with memcached
innovation: 145k-node botnet from
hacking IoT devices

The Need for Better DDoS Defenses

- Source address filtering…

  good, but a goal since 2000 *(RFC2267)*

- Filtering and scrubbing at the target…

  good, but not vs. 1Tb/s

- CDN services…

  great, but can be expensive

Our goal: best-of-breed DDoS defense, and open-source

PAADDoS: Who We Are

Leandro Bertholdo,
U. Twente

João Ceron,
U. Twente

John Heidemann,
USC/ISI, PI

Yuri Pradkin,
USC/ISI

Aiko Pras,
U. Twente, PI

Lan Wei,
USC/ISI

Wouter de Vries.
U. Twente

USC Viterbi School of Engineering
Information Sciences Institute

UNIVERSITY OF TWENTE.

ant.isi.edu

data distribution
support through
DHS/IMPACT

impact Cyber Trust
www.impactcybertrust.org

collaboration with

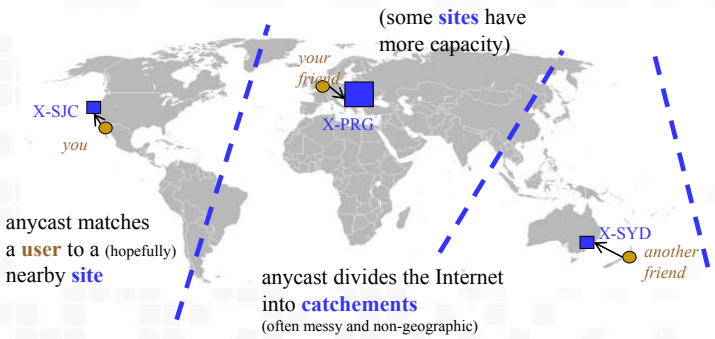
SIDN LABS

USC University of Southern California

B Root

Our Approach: Democratizing Anycast

- Replication of the service … **anycast**
  - multiple physical sites
  - BGP matches users to sites
  - spreads load over sites
- Anycast is widely used but it is a black art
- Our goal: document and democratize anycast



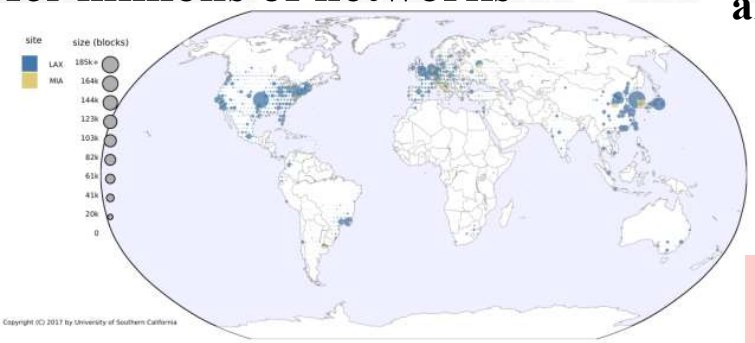
PAADDOS Objectives

- **Map cachements** with active probing with Verfploeter
- **Plan for changes** with new tools
- **Support reconfiguration** during attack
- **Evaluate and document** these ideas

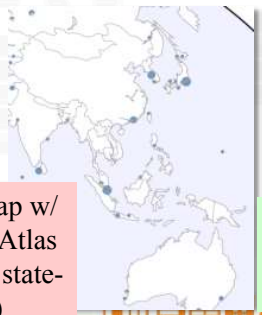
Early Results: Verfplotter Anycast Mapping

Verfplotter idea: use active probing to map anycast

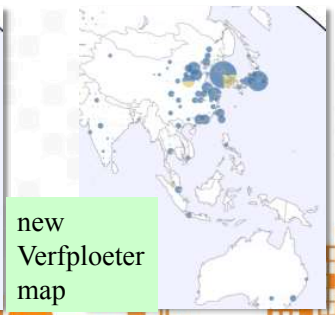
Result: a **global picture** for **millions of networks**



better coverage, in South America **and in China and Korea** (below)



old map w/ RIPE Atlas (prior state-of-art)



new Verfploeter map

Benefits: Better Defenses Against DDoS

- Document use of anycast to support smaller players
- Publish best practices
- New open-source tools that anyone can use

- Goal:
  - Broaden the field of defenders
  - Share practices that are today often closed

Collaboration and Competition

- Current methods: *good, but not enough*
  - source-address validation: *deployment remains incomplete*
  - new filtering techniques: *complement our approach*

- Commercial DDoS defense providers and CDNs
  - great for those who pay for them
  - should not be the *only* option

PAADDoS: Current Status and Next Steps

Current status

- Kick-off meeting and discussion at NCSC ONE in October 2018
- Formally underway in November 2018
- Verfploetter anycast mapping available today
  - https://ant.isi.edu/software/verfploeter/

Plans

- Examine long-term Verfploeter data
- Develop planning tools

Tech Transition Activities

- Verfploeter already in operation at B-Root and a major anycast DNS operator
- Continue work with operators
  - SIDN Labs (Netherlands), operate .nl
  - B-Root (USC), one of the 13 root servers
- Discussions with many other operators
- Code and approaches will be open source

Conclusions and Contact Info

- anycast as a DDoS defense
  - not new
  - but new understanding and docs
- mapping with Verploeter
  - working with multiple DNS operators
- new tools to plan before and react during attacks
  - (in progress)

Contact Info

John Heidemann
USC-ISI
johnh@isi.edu

Aiko Pras
University of Twente
a.pras@utwente.nl

https://ant.isi.edu/paddos/