GrayStar

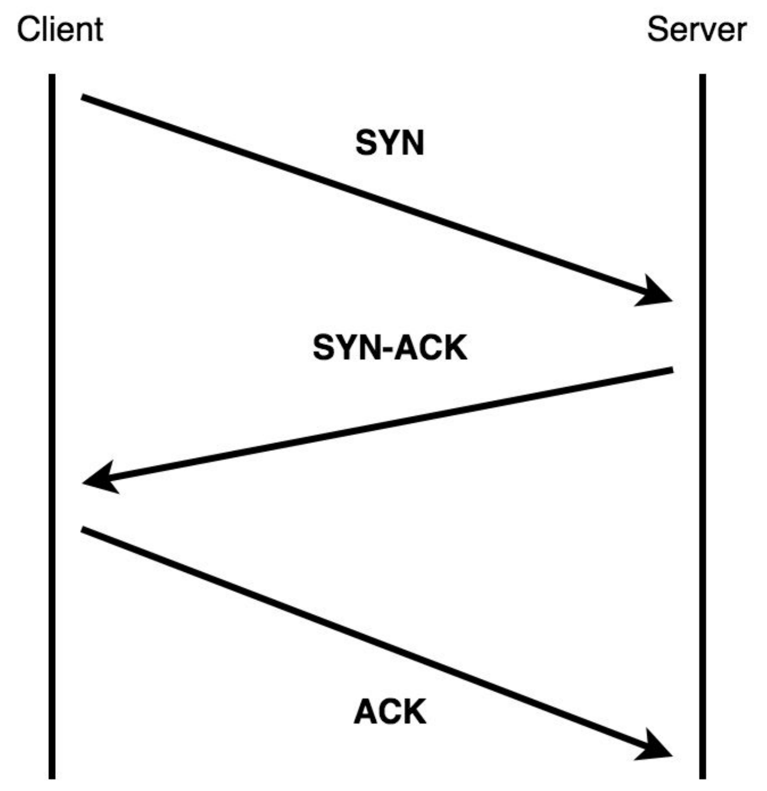
Shayan Javid, Genevieve Bartlett
Information Sciences Institute
shayanjavid07@g.ucla.edu, bartlett@isi.edu

Introduction

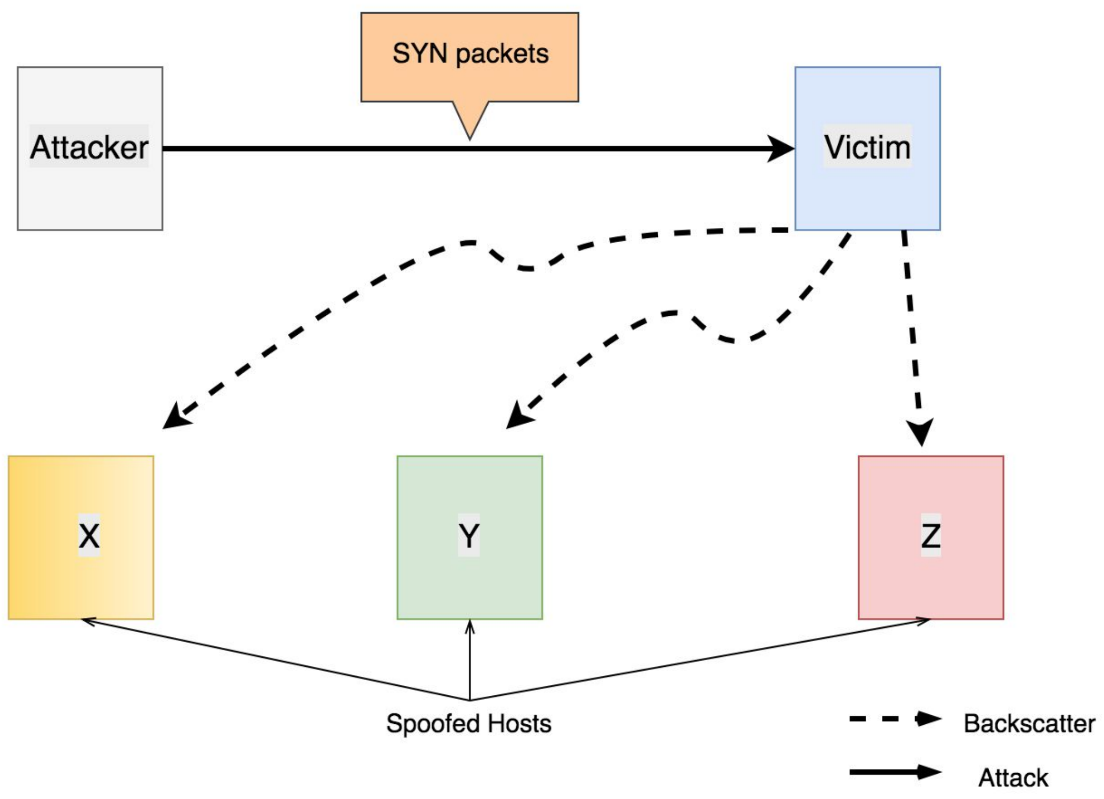
- Darknet (network telescope) is an approach to observe large-scale events on the Internet by observing traffic going to unused (dark) address spaces in networks
  - Observe unsolicited traffic
  - Collect information on different phenomena such as denial-of-service attacks, backscatter, worm propagation, and misconfigurations
- GrayStar:
  - Use the idea of network telescopes but build a framework that a group of volunteers would run on their local machines to collect and report unsolicited traffic
- Challenges:
  - Developing methods to enable privacy-preserving sharing of observed events from our volunteers
  - Developing a reliable method to capture unsolicited packets headed towards open ports on a device

Background

- TCP Three-Way Handshake



- Backscatter



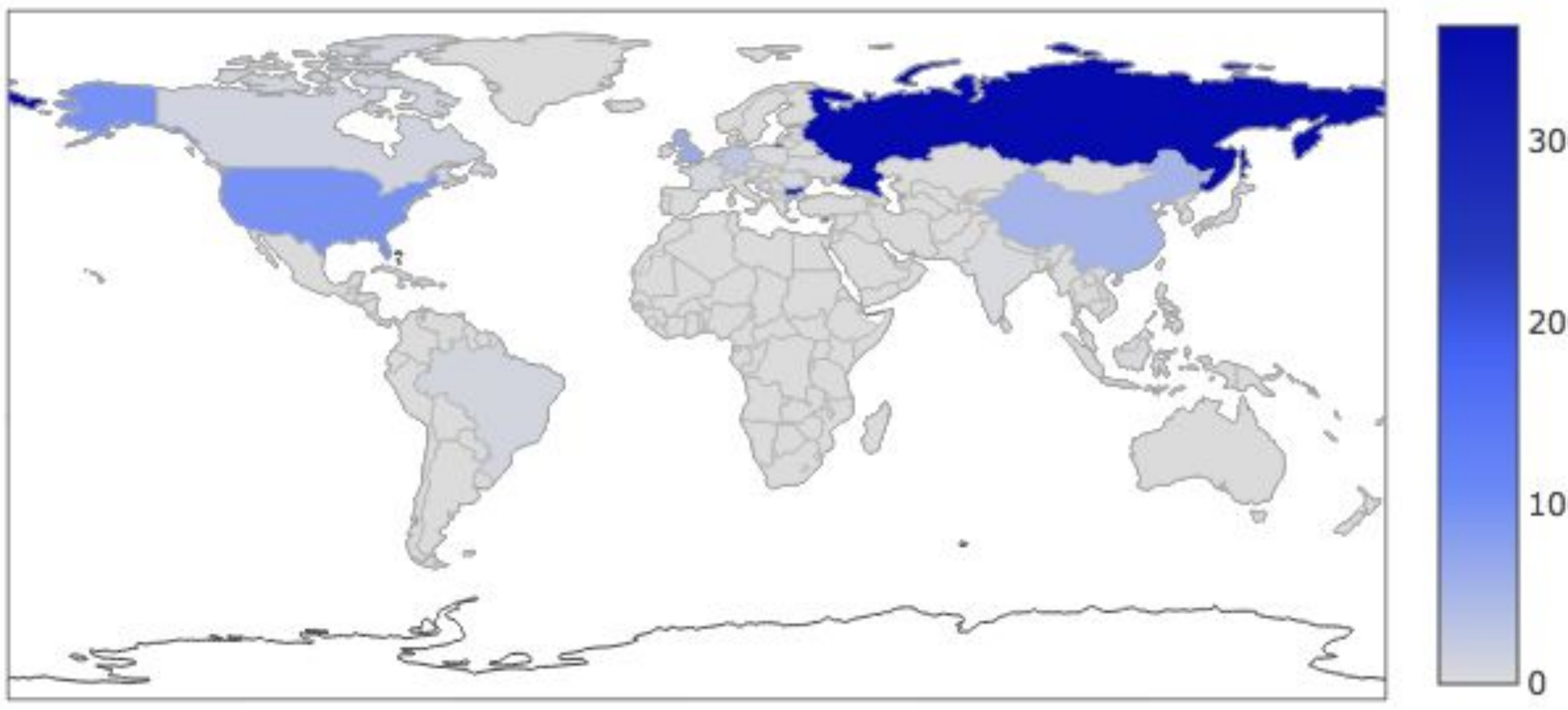
Detecting Unsolicited Traffic

- In order to detect the unsolicited traffic, first we get information on the device's open or closed ports
- Any packet towards the closed ports is considered unsolicited
- Determining a reliable method to distinguish the unsolicited traffic from the solicited one for the open ports is our next step

Network Telescope vs GrayStar

- GrayStar can be used by any researcher, while a network telescope requires one to own a sufficiently large unused address space
- Using GreyStar we can study diverse unsolicited traffic contributed by many volunteers from many devices, while a network telescope only observes traffic to one unused space
- Most of the unused address spaces are now known to attackers, so they can avoid being observed by network telescopes

Evaluation



The choropleth above displays every country that we receive unsolicited packets from in our observation on a single device on ISI's network.

- This monitoring has been done on a single device using our framework for 11 hours on the ISI's network
- During our observation we captured 1051 TCP-SYN packets
- From these 1051 packets only 470 had unique source IP addresses
- In our observation we discovered 2 Russian bots constantly scanning our device looking for open ports
- We captured 364 TCP-SYN packets from Russia with only 38 unique IP addresses. Which means that,on average, we captured 9 unsolicited packets from a single IP address

If interested contact <Shayan Javid> shayanjavid07@g.ucla.edu
Project Web page: <github.com/gbartlet/Graystar>

Work performed under REU Site program
supported by NSF grant #1659886

USC Viterbi
School of Engineering
Information Sciences Institute