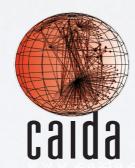
# Measuring and Monitoring BGP

Alberto Dainotti, alberto@caida.org



Center for Applied Internet Data Analysis University of California, San Diego

Why?

### BGP is the central nervous system of the Internet

BGP's design is known to contribute to issues in:

### Availability

- -Labovitz et al. "Delayed Internet Routing Convergence", IEEE/ACM Trans. Netw., 2001.
- -Varadhan et al. "Persistent Route Oscillations in Inter-domain Routing". Computer Networks, 2000.
- -Katz-Bassett et al. "LIFEGUARD: Practical Repair of Persistent Route Failures", SIGCOMM, 2012.

### Performance

-Spring et al. "The Causes of Path Inflation". SIGCOMM, 2003.

### Security

-Zheng et al. "A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Realtime". SIGCOMM, 2007.

### Need to engineer protocol evolution!



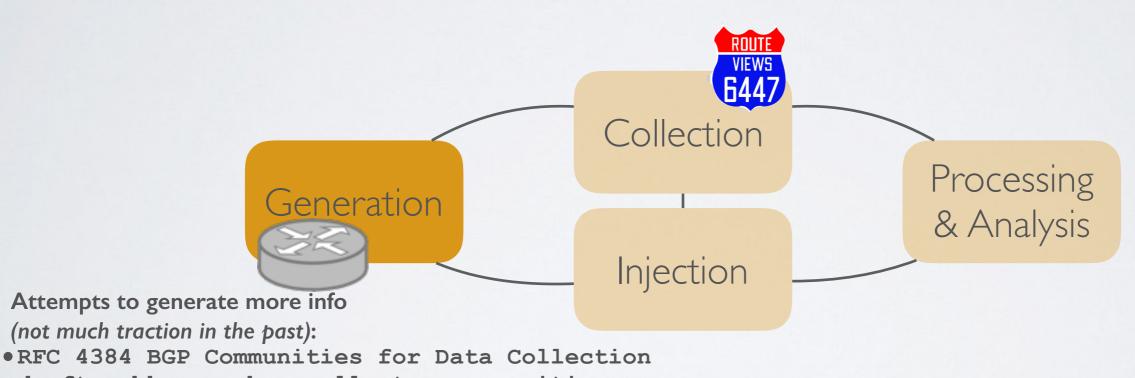
### Why?

Defining problems and make *protocol* engineering decisions through realistic evaluations is difficult also because we know little about the <u>structure</u> and <u>dynamics</u> of the BGP ecosystem!

- AS-level topology
  - -Gregori et al. "On the incompleteness of the AS-level graph: a novel methodology for BGP route collector placement", IMC 2012
- AS relationships
  - -Giotsas et al. "Inferring Complex AS Relationships", IMC 2014
- AS interactions: driven by relationships, policies, network conditions, operator updates
  - -Anwar et al. "Investigating Interdomain Routing Policies in the Wild", IMC 2015
  - -Lychev et al. "BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?", SIGCOMM 2013

### two issues - somehow related

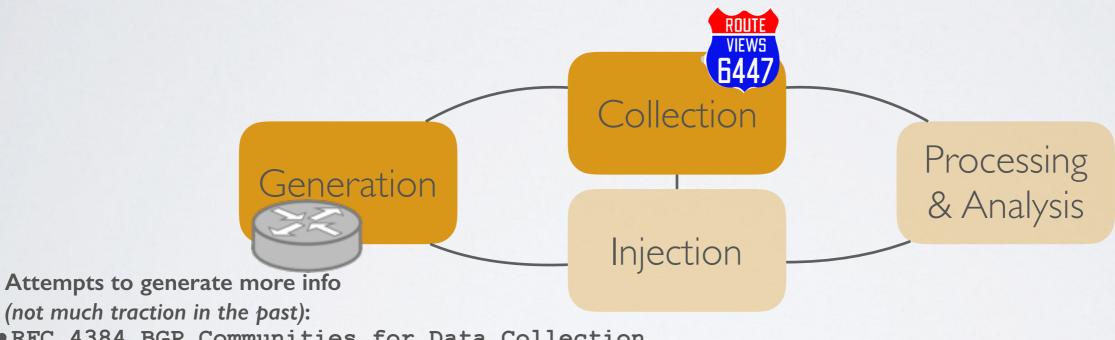
- I. Literature shows that we need more/better data
  - more info from the protocol/routers





### two issues - somehow related

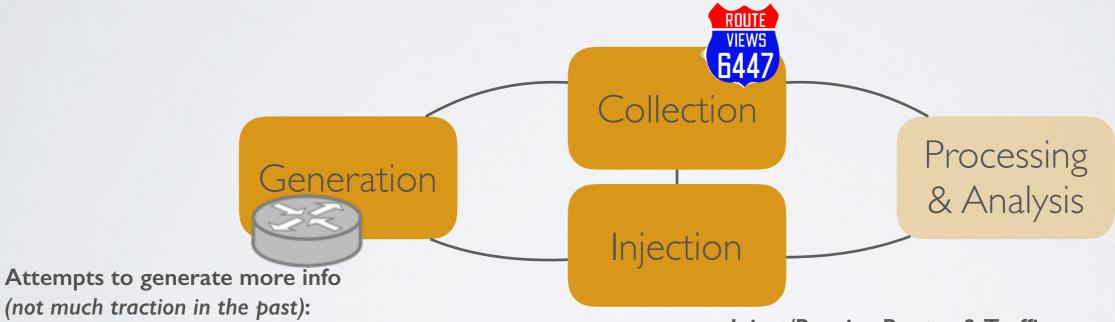
- I. Literature shows that we need more/better data
  - more info from the protocol/routers, more collectors,



- RFC 4384 BGP Communities for Data Collection
- draft-ymbk-grow-bgp-collector-communities

### two issues - somehow related

- I. Literature shows that we need more/better data
  - more info from the protocol/routers, more collectors, more experimental testbeds, ...



•RFC 4384 BGP Communities for Data Collection

• draft-ymbk-grow-bgp-collector-communities

Inject/Receive Routes & Traffic.
PEERING - http://peering.usc.edu
Schlinker et al. "PEERING: An AS for Us", HotNets 2014



### two issues - somehow related

- I. Literature shows that we need more/better data
  - more info from the protocol/routers, more collectors, more experimental testbeds, ...
- 2. But we also need better tools to learn from the data
  - to make data analysis: easier, faster, able to cope with BIG and heterogeneous data
  - to monitor BGP in near-realtime
  - tightening data collection, processing, visualization, ...



## BGP EVENTS & DYNAMICS

IODA: Detection and Analysis of Internet Outages

 Country-level Internet Blackouts during the Arab Spring

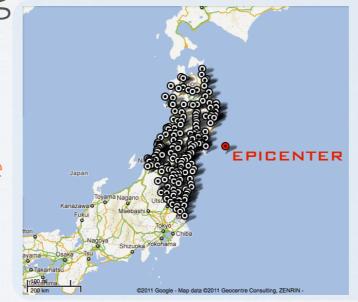
> Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship" IMC 2011



EGYPT, JAN 2011 GOVERNMENT ORDERS TO SHUT DOWN THE INTERNET

 Natural disasters affecting the infrastructure

Dainotti et al. "Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet" SIGCOMM CCR 2012



JAPAN, MAR 2011 EARTHQUAKE OF MAGNITUDE 9.0





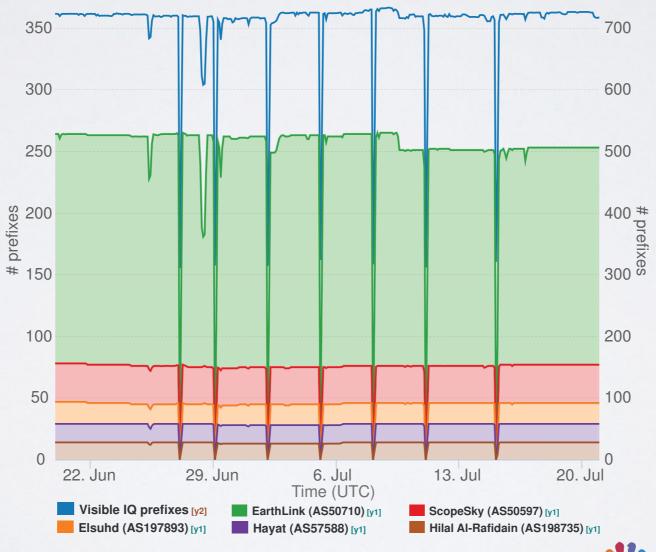


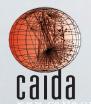


## BGP EVENTS & DYNAMICS

### IODA: Detection and Analysis of Internet Outages

Country-wide Internet outages in Iraq that the government ordered in conjunction with the ministerial preparatory exams - Jul 2015







## BGP EVENTS & DYNAMICS

### IODA: Detection and Analysis of Internet Outages

Outage of AS11351(Time Warner Cable LLC) September 30, 2015









### BEFORE IODA

### post-event manual analysis



EGYPT, JAN 2011
GOVERNMENT ORDERS
TO SHUT DOWN THE
INTERNET



4 months of work



Dainotti et al. "Analysis of Country-wide Internet Outages Caused by Censorship" IMC 2011



Center for Applied Internet Data Analysis University of California San Diego

### Analysis of Country-wide Internet Outages Caused by Censorship

Alberto Dainotti University of Napoli Federico III alberto@unina.it Claudio Squarcella. Roma Tre University squarcel@dia.uniroma3.it

Emile Aben RIPE NCC emile.aben@ripe.net

Kimberly C. Claffy CADA UCSD kc@caida.org Marco Chiesa Roma Tre University chiesa@dia.uniroma3.it

Michele Russo Antonio Pescapé rsity of Napoli Federico II University of Napoli Federico

### ABSTRACT

In the time rounds of rapid in several North presents and threats of of these disruptions for the ratios on analytic is to academic researched date, amothered profess and buddient seek country, on exit to BGF amounted using public amounted trape. We then analyzed profess and ASon three, country plane and date to amount of the amount of the country alone and date to disconnection. Our med dates country of accountry of the country of a trapeling or similar goognafies or trapelings.

### Categories and 5 C23 [Noteork Opera C23 [Local and Wide

General Terms

Mourannest, Socurity

Personner or make digit presented or distributed to not made or distributed to hear this nation and the ful impallied, to post on surva personners and/or a fur DACTA, Nevember 2-4, 2 Coppright 2011 ACM 978

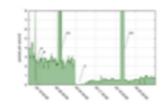


Figure 12: UCSD dishear's realis coming from Libya Labels A, B. C indicere the three contages. Spilon labeled D1 and D2 are that to backworker from two denial of nervice attacks.

related to protects in the country. The web site of the Ministry of Communications (seeing recog) was attacked with a randomly-specified Dod attack just before the outage stated, on humany 25 of different since: 15 of OMT (10 to manuscs), 10 55 OMT (17 manuscs), and 21 99 OMT (35 manuscs), and 21 99 OMT (35 manuscs), and 21 99 OMT (35 manuscs), analysis of the hardson offers at tack to terms of public size, indicating average pucket main between 21k and 15k puckets page uses of the public size.

On Polymery 2 the such size of the Egyptian Ministry of Interior inconsisting property was trapeted by two BVS strake, just the tie the end of the consorting leven 11-07 to 17-29 GMT and the 17-08 to 17-17 GMT. The cases SF address was straked another time the day after, from 10-08 to 08-12 GMT. In this case the conmantal goods rems was considered, resumed To-posture personnel.

### 5.2 Libya

### 521 Overview

Libya's historic influence or one more posse to manipulation than Egypt's, pudging from its physical structure from Egypt's, pudging from its physical structure from minimal community; is provided by only two substantial collects, both and/ug in Tipod [39], and the homeon influence test in dominated by a single, state owned. AS: We only found two other ASiachaving a small prosence in Libya, in described in European 1.2.2.

In Libya three different entages in early 2011 were identified.

In Libya three different estages in endy 2011 were simulated and publicly documented (Figure 13, Figure 12, shows the miffle observed by the UCED retwork telescope from Libya froughout an interval measureming the entages. The govern billion of Government of Conferent three-different blocker quicodes; prom Bil and GS offer to two-densitied of service estages discussed in Section 5.2.3. Toward the right of the graph it is difficult to interpret what in really happening in Libya because of the civil was.

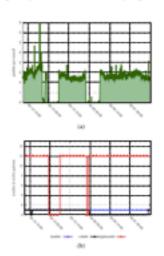
### 5.2.2 Ownger in detail

The first two outages happened during two consecutive nights. Figure USGs shows a recer detailed view of these two outages as absured by the USES takescope. Figure 15(b) shows BCF data over the same arrands in both cases, within a few animates, 12 out of the 15 Hy4 positions received with FP address reages officially deligated to Libys were withfarran. These twelve IFv4 positions were actually to be local volumes appearing Alexander animates of the summaring IFv4 position was managed by BAASE. As of May 2011, there were no IFv6 positions on Advides Oxfore posit 21 one-configures IF surges in Libys, off post of an excenquening IFv6.

prefix agreement by SotASI, which provides satellite services in the Middle East, Asia and Africa The convening PlvI prefix also contrained 180 Pragas on accord other countries produces arrively in the Middle East. We considered the additional AI because the UCSD desired guarantly desired a splitting arrange of unsohelded traffic contain from Plv in those IZ ranges before the fixed owing inform NN pushess such day The level of Paskgroundired. It indicates a population of convenient using PCs Middly indicated by Contribute or other malware, allowing infrances of network condition. Traffic from this network also provided existence of what happened to Lidyan Entered agreements haved on usualitie systems are managed by the local sixtences provided.

and managed by the hood relacion procedur.

Comparing Figures 15th and 15th receive a different behavior that conflicts with previous respects [17], the second outage was not noticely consord by BGP withstreads. The BGP distallment began on February 19 around 21 50 35 UTC, exactly matching the sharp discrete of distinct ineffic from Liftys cond in accordance with reports on Liftys in traffic seen by Arber Network [35] [blust or midel approximately one hour lates, at 25 05 32. In contrast, the latenace outage on closes by the telecopous data and reported by the news [17]
leasted until approximately February 26 at 6.12 UTC. This finding suggests that a different desagries to the stage — a pudel-blocking strongy approxemity adopted autosportely in the third categor and acceptance of the first outside strongy approximately for the world it was already being and discrepation for the world it was already being and dis-

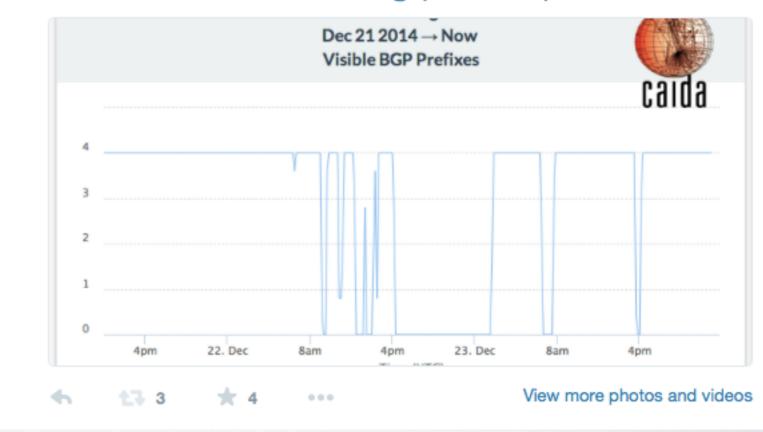


## IODA TODAY

### live Internet monitoring

Last Christmas we made it possible for anybody to follow the North Korean disconnection almost live







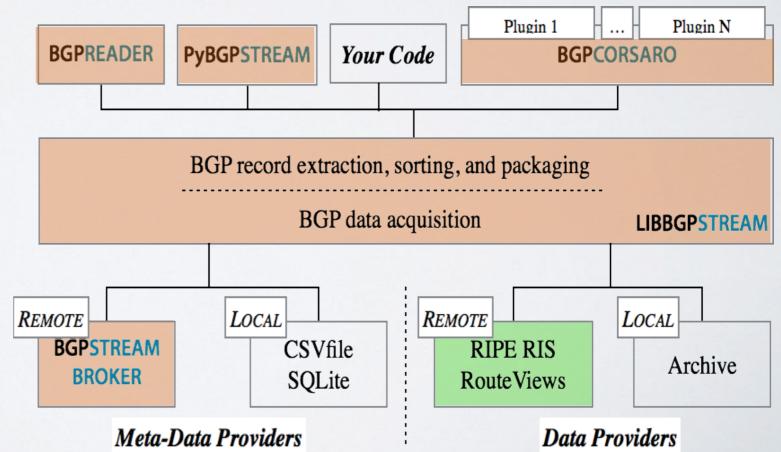
### two issues - somehow related

- I. Literature shows that we need more/better data
  - more info from the protocol/routers, more collectors, more experimental testbeds, ...
- 2. But we also need better tools to learn from the data
  - to make data analysis: easier, faster, able to cope with BIG and heterogeneous data
  - to monitor BGP in near-realtime
  - tightening data collection, processing, visualization, ...





- A software framework for historical and live BGP data analysis
- Design goals:
  - -Efficiently deal with large amounts of distributed BGP data
  - -Offer a time-ordered data stream of data from heterogeneous sources
  - -Support near-realtime data processing
  - -Target a broad range of applications and users
  - -Scalable
  - -Easily extensible

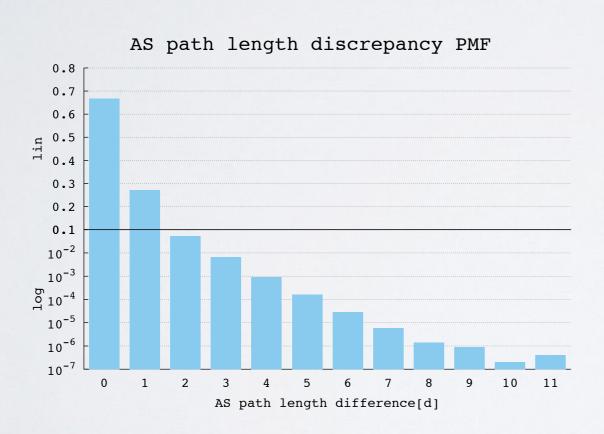


Center for Applied Internet Data Analysis University of California San Diego

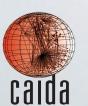
### PYBGPSTREAM

### Example: studying AS path inflation

How many AS paths are longer than the shortest path between two ASes due to routing policies? (directly correlates to the increase in BGP convergence time)



```
from _pybgpstream import BGPStream, BGPRecord, BGPElem
from collections import defaultdict
from itertools import groupby
import networkx as nx
stream = BGPStream()
as graph = nx.Graph()
rec = BGPRecord()
bgp_lens = defaultdict(lambda: defaultdict(lambda: None))
stream.ad _filter('record-type','ribs')
                                                                                      10
stream.ad_interval_filter(1438415400,1438416600)
                                                                                      11
stream.st rt()
                                                                                      12
                                                                                      13
                                                                                      14
while(str am.get_next_record(rec))
                                                                                      15
    elem rec.get_next
    while elem):
                                                                                      16
                                                                                      17
                                                                                      18
            = [k for k, g in groupby(elem.fields['as-path'].split(" "))]
                                                                                      19
            origin = hops[-1]
                                                                                      20
            for i in range(0,len(hops)-1):
                                                                                      21
                as_graph.add_edge(hops[i],hops[i+1])
                                                                                      22
            bgp_lens[monitor][origin] = \
                                                                                      23
               min(filter(bool,[bgp_lens[monitor][origin],len(hops)]))
                                                                                      ^{24}
       elem = rec.get_next_elem()
                                                                                      25
for monitor in bgp_lens:
                                                                                      26
                                                                                      27
   for origin in bgp_lens[monitor]:
                                                                                      28
       nxlen = len(nx.shortest_path(as_graph, monitor, origin))
       print monitor, origin, bgp_lens[monitor][origin], nxlen
                                                                                      29
```

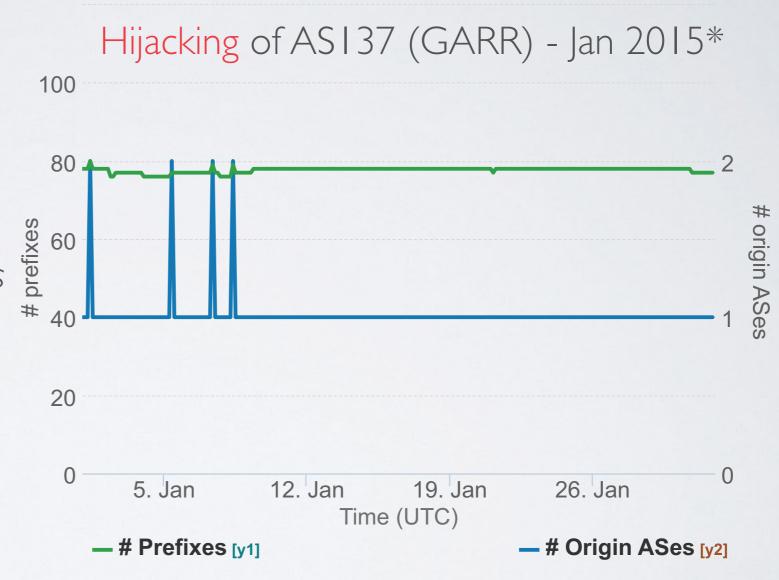


## BGPCORSARO

### Example: monitor your own address space on BGP

The "prefix-monitor" plugin (distributed with source) monitors a set of IP ranges as they are seen from BGP monitors distributed worldwide:

- how many prefixes reachable
- how many origin ASes
- generates detailed logs

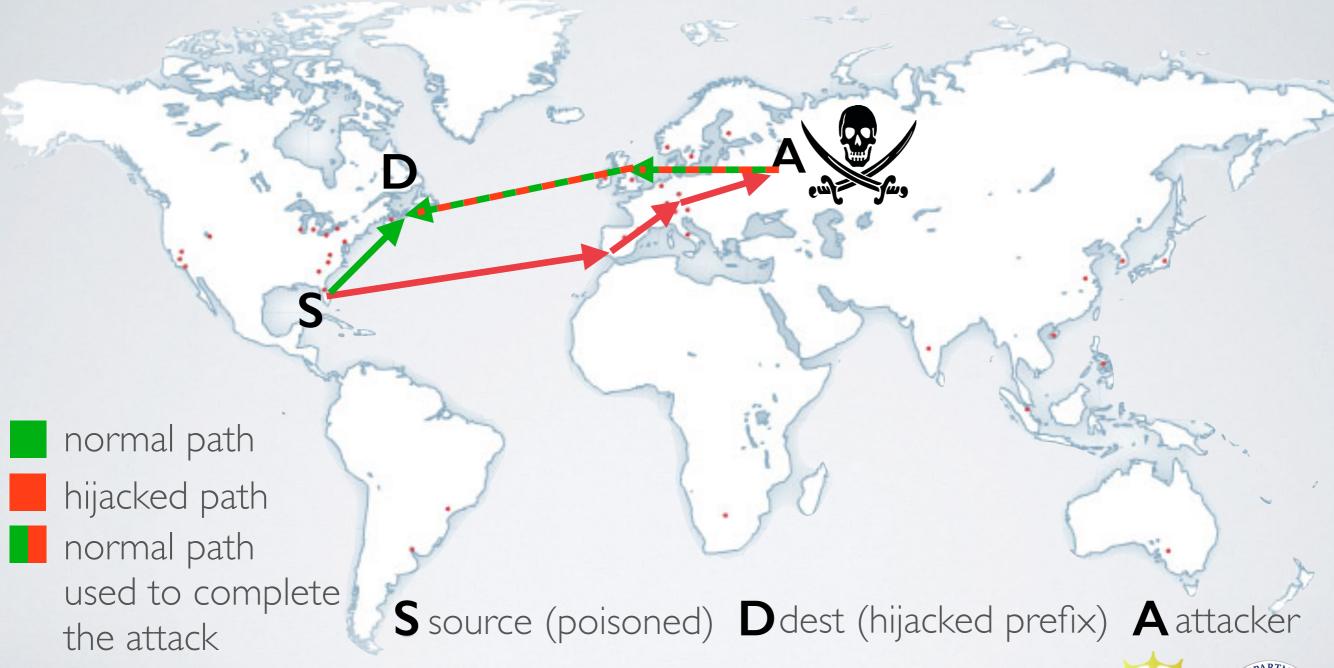




\*Originally discovered by Dyn: http://research.dyn.com/2015/01/vast-world-of-fraudulent-routing/

# ANOTHER SUPPORTED PROJECT

Hijacks: detection of MITM BGP attacks









# ANOTHER SUPPORTED PROJECT

Hijacks: detection of MITM BGP attacks

Research informed by (and tested with) data in the wild

Data-plane active measurements

Live BGP measurements trigger on-demand dataplane measurements (e.g., traceroutes) during a suspicious event.







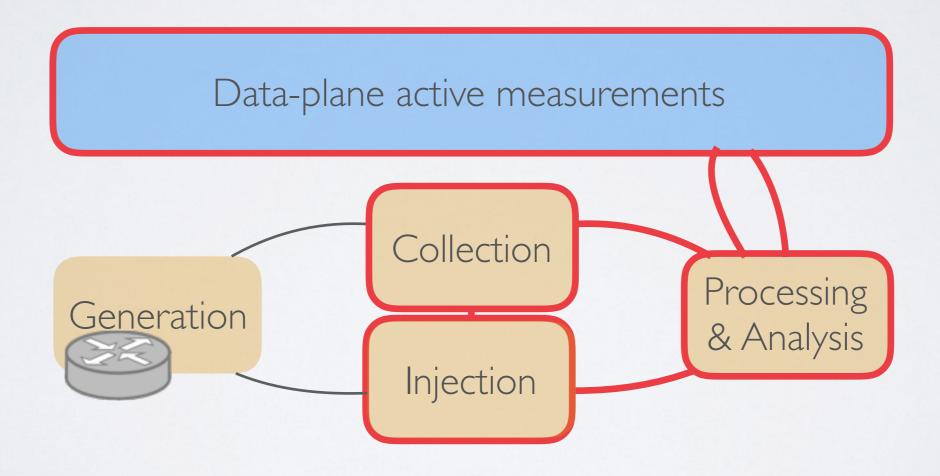




## BGP HACKATHON - FEB 2016

theme: "live BGP measurements & monitoring"

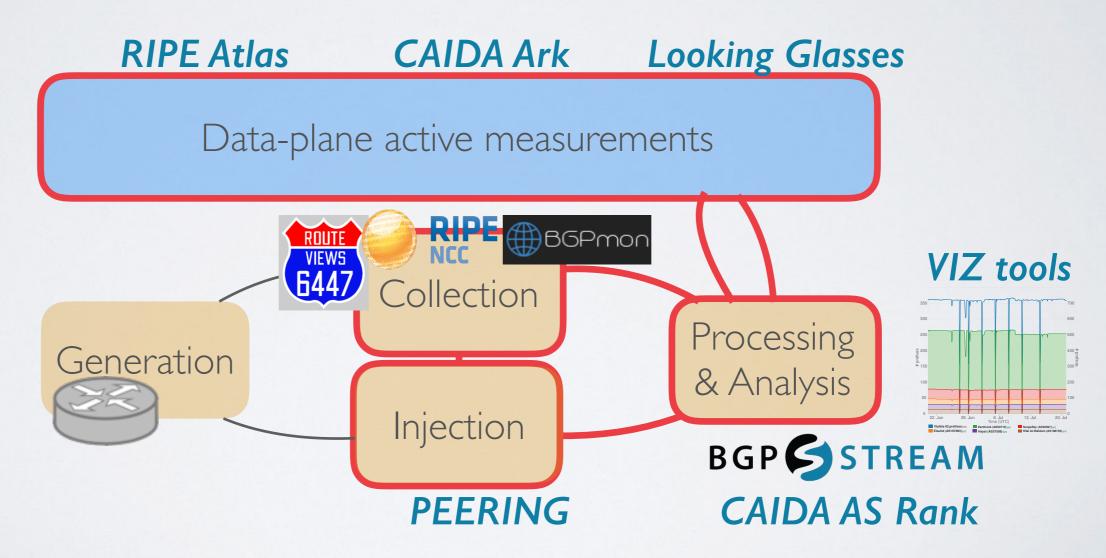
Improve/Integrate tools to study the BGP eco-system. Target practical problems: topology, hijacks, outages, RPKI deployment, path inflation, circuitous paths, policies, relationships, visualize dynamics, ...

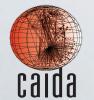


### BGP HACKATHON - FEB 2016

theme: "live BGP measurements & monitoring"

We will provide a rich toolbox and "live" data access:





### BGP HACKATHON

http://github.com/CAIDA/bgp-hackathon/wiki

- •6-7 February 2016 (weekend before NANOG 66)
- · San Diego Supercomputer Center, UC San Diego
- Theme: live BGP measurements and monitoring
- Toolbox: BGPMon, RIPE RIS, PEERING, BGPStream, RIPE Atlas, CAIDA Archipelago, Route Views, looking glasses, AS relationships, AS Rank, Visualization tools, ...



- join us and come over to hack!
- help teams as a domain expert
- propose projects that hacking teams may pick
- offer to join the jury that will assign awards

>>> bgp-hackathon-info@caida.org <<<



















## THANKS

<u>bgpstream</u>.caida.org github.com/CAIDA/bgp-<u>hackathon</u>/wiki

