ARTEMIS: Real-Time Detection and Automatic Mitigation for BGP Prefix Hijacking

Gavriil Chaviaras[1,2], Petros Gigis[1,2], Pavlos Sermpezis[1], and Xenofontas Dimitropoulos[1,2]

{gchaviaras, gkigkis, sermpezis, fontas}@ics.forth.gr

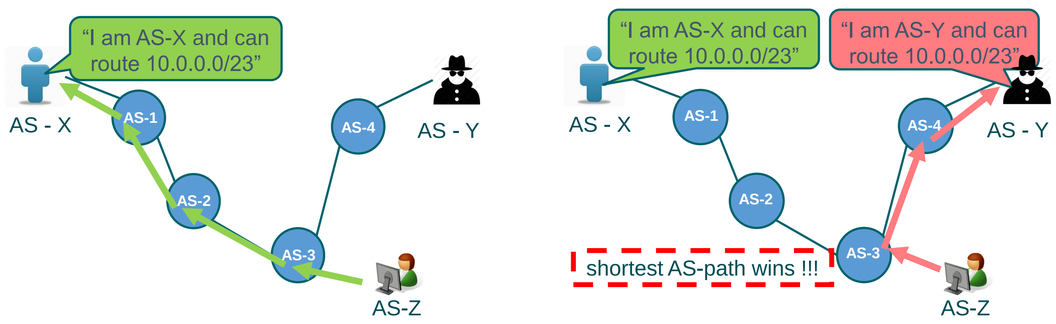
[1] FORTH, Greece [2] University of Crete, Greece

1. Background and Motivation

- The Border Gateway Protocol (BGP) is a distributed protocol without –globally deployed– authorization mechanisms.
- An Autonomous System (AS) can announce illegitimate BGP paths, *hijacking* thus IP prefixes of other ASes.
- BGP Prefix Hijacking is a common phenomenon in the Internet that can cause serious routing problems and economic losses.

Examples of public/notorious BGP hijacking cases

- Hackers performed several short hijacks, through a Canadian ISP, and stole *~$100k* bitcoins in 2014.
- A Chinese ISP mistakenly announced *15%* of the entire BGP table in 2010.
- An ISP in Pakistan, due to a misconfiguration, hijacked YouTube's prefixes and disrupted its services for *2* hours in 2008.



State-of-the-art detection & mitigation mechanisms:

Most existing solutions are "third-party" alert systems that introduce significant delay until the mitigation of a prefix hijacking.

- Third-party detection services watch the entire BGP table.
- Network administrators need to manually verify a hijack alert.
- Manual reconfiguration of routers are needed to mitigate the hijack.

➢ The total time needed is several minutes to a few hours.

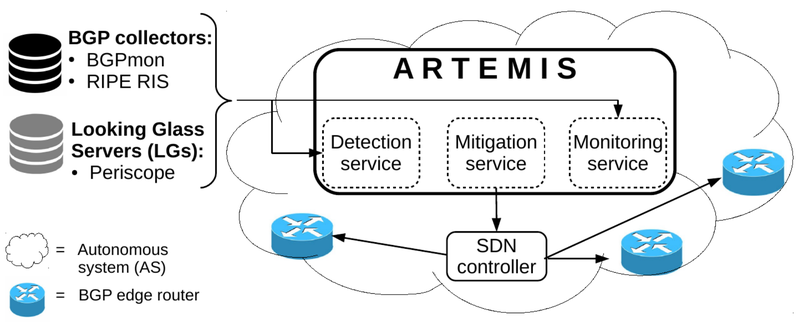
➢ This is too slow; especially since more than 20% of hijacks last <10min.

2. Our solution: ARTEMIS

*(**A**utomatic and **R**eal **T**ime d**E**tection and **MI**tigation **S**ystem)*

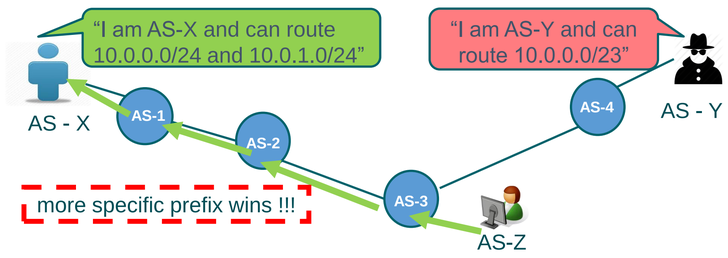
Key Features

- Monitoring: many vantage points & light-weight.
- Detection: real-time & no false positives.
- Mitigation: automatic (e.g., over SDN controller) & fast.



ARTEMIS Overview

- A system that is used by an AS to detect & mitigate hijacks against its *own* prefixes. (not a third-party service; no false positives)
- Detection is based on BGP data from public control-plane sources:
  - Route collectors (BGPmon & RIPE RIS streaming interfaces)
  - Looking Glass servers (through the Periscope tool)
- Mitigation uses *prefix de-aggregation*: the affected AS immediately announces sub-prefixes of the hijacked prefix.



3. Experiments with a real AS

The *PEERING* testbed (https://peering.usc.edu/)

- Owns real ASNs and IP prefixes.
- Has servers at different sites around the world (IXPs, universities, etc.).
- Peers with real networks.
- Users can announce IP prefixes, through BGP, to the real Internet.

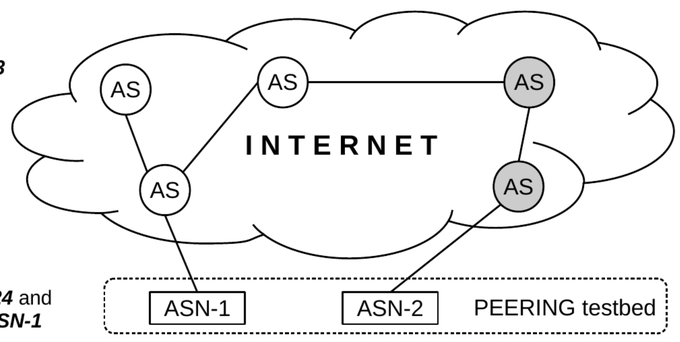
Experiments Setup

- ***Phase-1 (Legitimate announcement)***: Announcement of an IP prefix, e.g., *10.0.0.0/23*, from a PEERING site *S1*, with *ASN-1* as the origin-AS.
- ***Phase-2 (Hijacking & Detection)***:
  (a) From a different PEERING site *S2*, announcement of the same prefix *10.0.0.0/23*, with *ASN-2* as the origin-AS (i.e., BGP hijacking).
  (b) ARTEMIS detects the hijacking, the first time it receives data from a control-plane source, for the prefix *10.0.0.0/23* with *ASN-2.*
- ***Phase-3 (Mitigation)***: Immediately after the detection, ARTEMIS triggers the announcement of the (de-aggregated) sub-prefixes *10.0.0.0/24* and *10.0.1.0/24* from *S1* with *ASN-1* as the origin-AS.

Phase 1: AS AS route ***10.0.0.0/23*** to ***ASN-1***

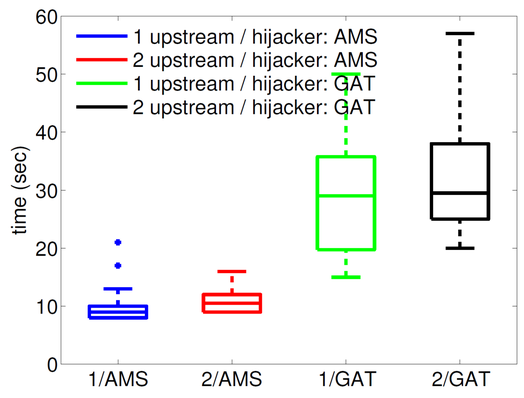
Phase 2: AS route ***10.0.0.0/23*** to ***ASN-1***; AS route ***10.0.0.0/23*** to ***ASN-2***

Phase 3: AS AS Route ***10.0.0.0/24*** and ***10.0.1.0/24*** to ***ASN-1***

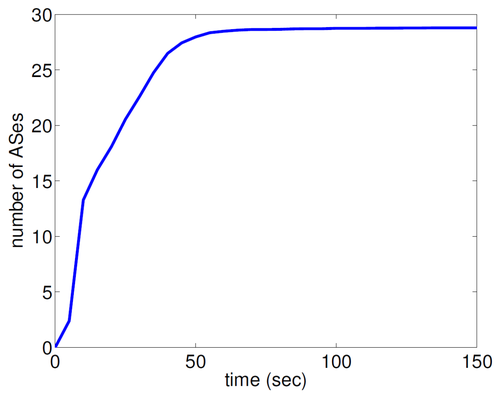


Measurements and Results

- Detection delay < 1min !
- From detection to mitigation (de-aggregation) 1-15sec !
- Mitigation completed (as seen from vantage points) ~5min !



Detection delay in different experiments presented in boxplots.



Process of mitigation: Number of ASes (as seen from the vantage points) switched to ASN-1, after the de-aggregation.

Control-plane sources / tools

- Periscope (http://www.caida.org/tools/utilities/looking-glass-api/)
- BGPmon (http://www.bgpmon.io/)
- RIPE RIS (http://www.ris.ripe.net/)

Acknowledgements

- This work has been funded by the European Research Council Grant Agreement no. 338402.

Contact Info

- We are the **INSPIRE Group**, and you can find us at:

http://www.inspire.edu.gr/

Follow @Inspire_Forth

ACM SIGCOMM, Florianópolis, Brazil, August 2016