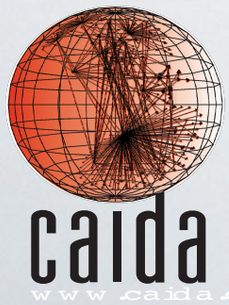
Neutralizing BGP Hijacking with the ARTEMIS Open-source Tool

Alberto Dainotti
alberto@caida.org
Center for Applied Internet Data Analysis
University of California, San Diego

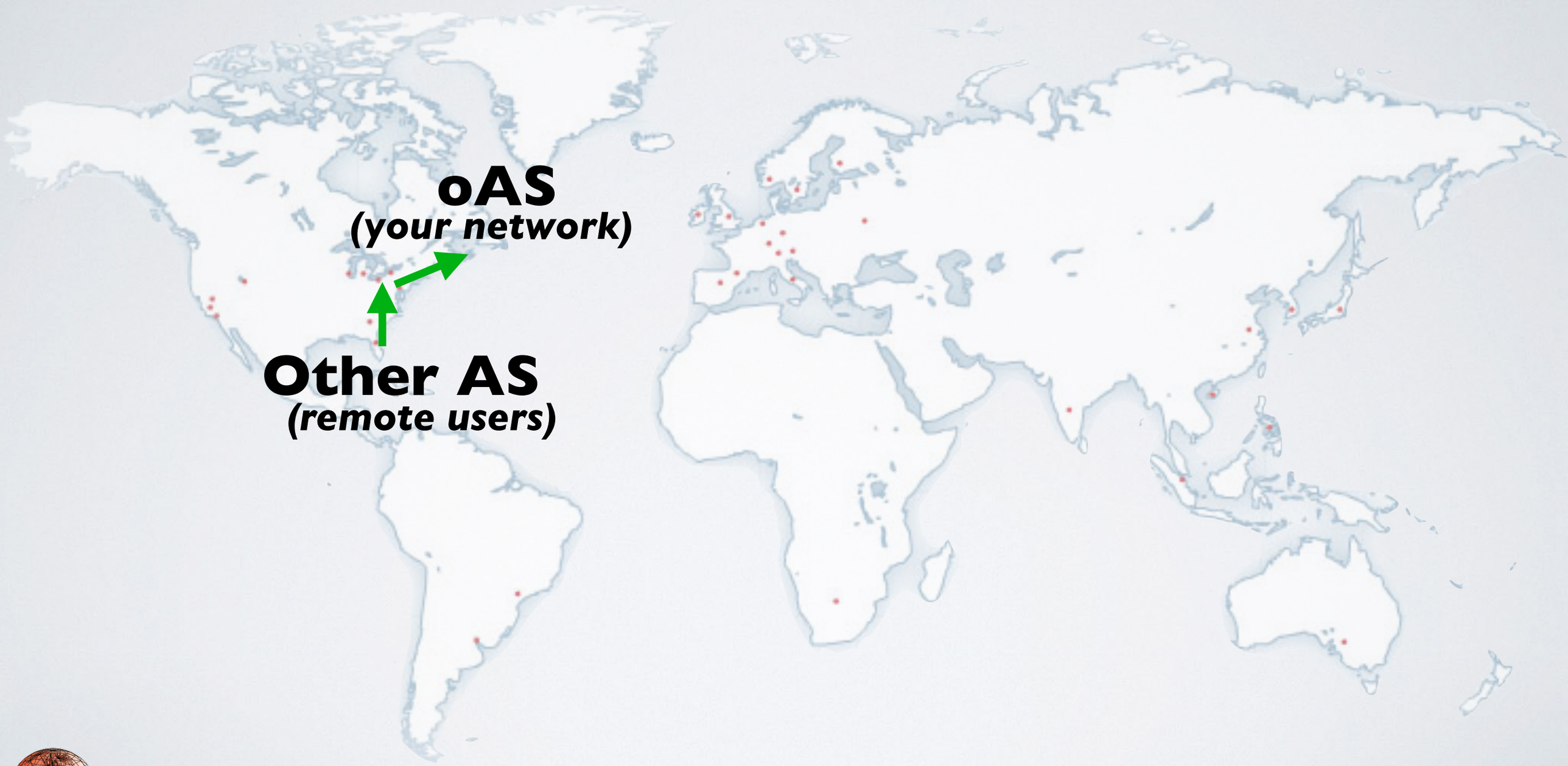
Joint work with:
Vasileios Kotronis, Dimitris Mavrommatis
Petros Gigis, Pavlos Sermpezis, Xenofontas Dimitropoulos, Alistair King, Mingwei Zhang



UC San Diego

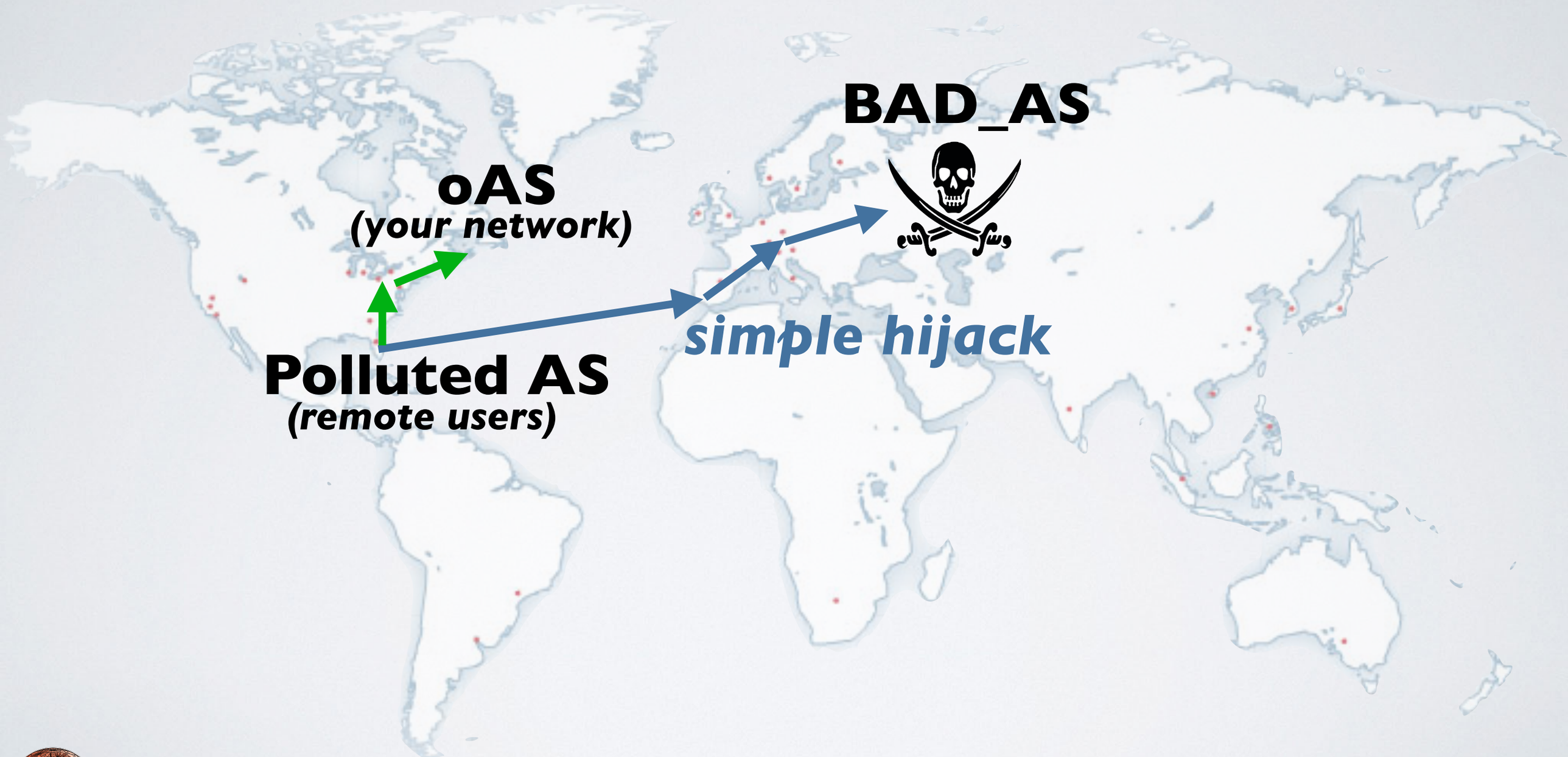
BGP HIJACKING

stealing/manipulating your routes



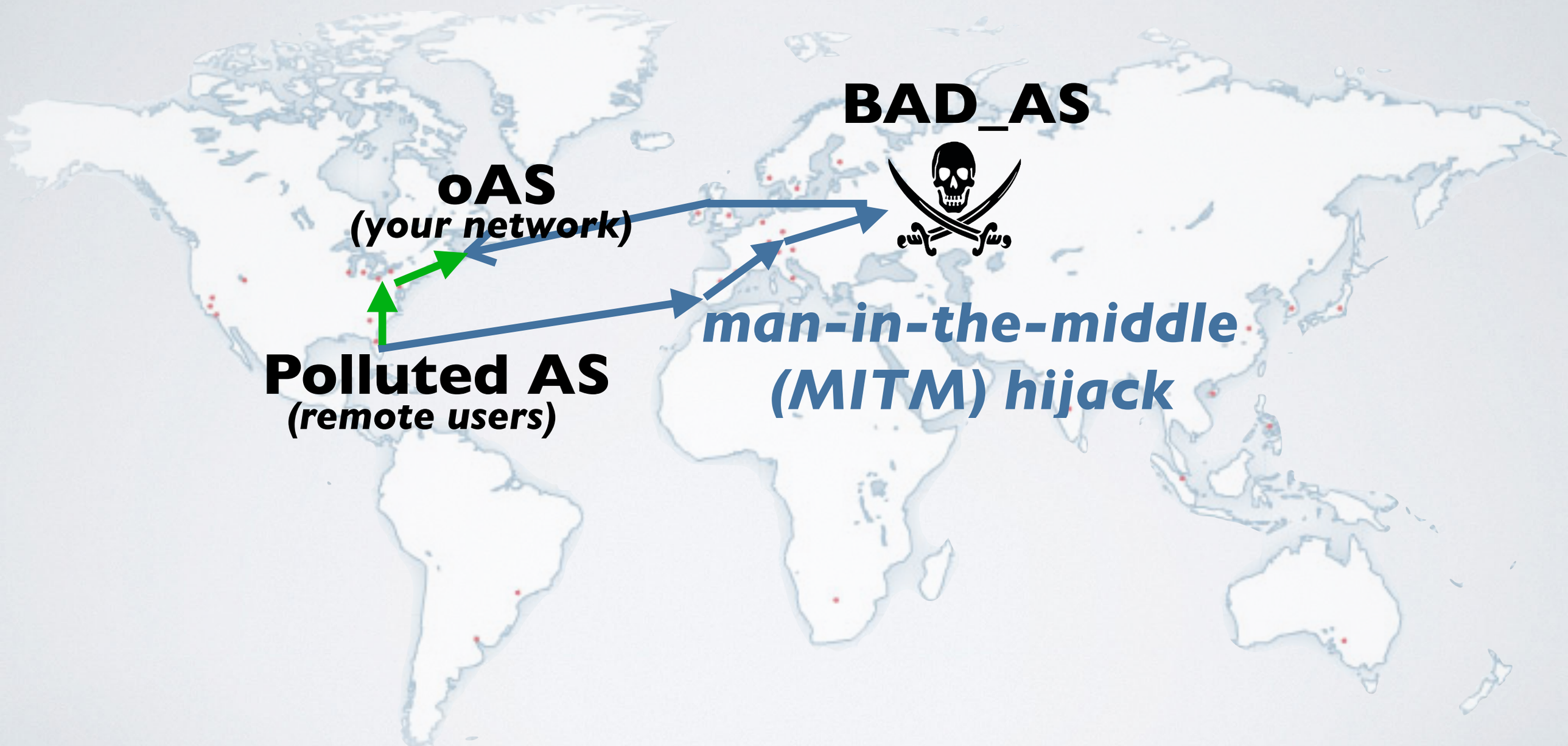
BGP HIJACKING

stealing/manipulating your routes



BGP HIJACKING

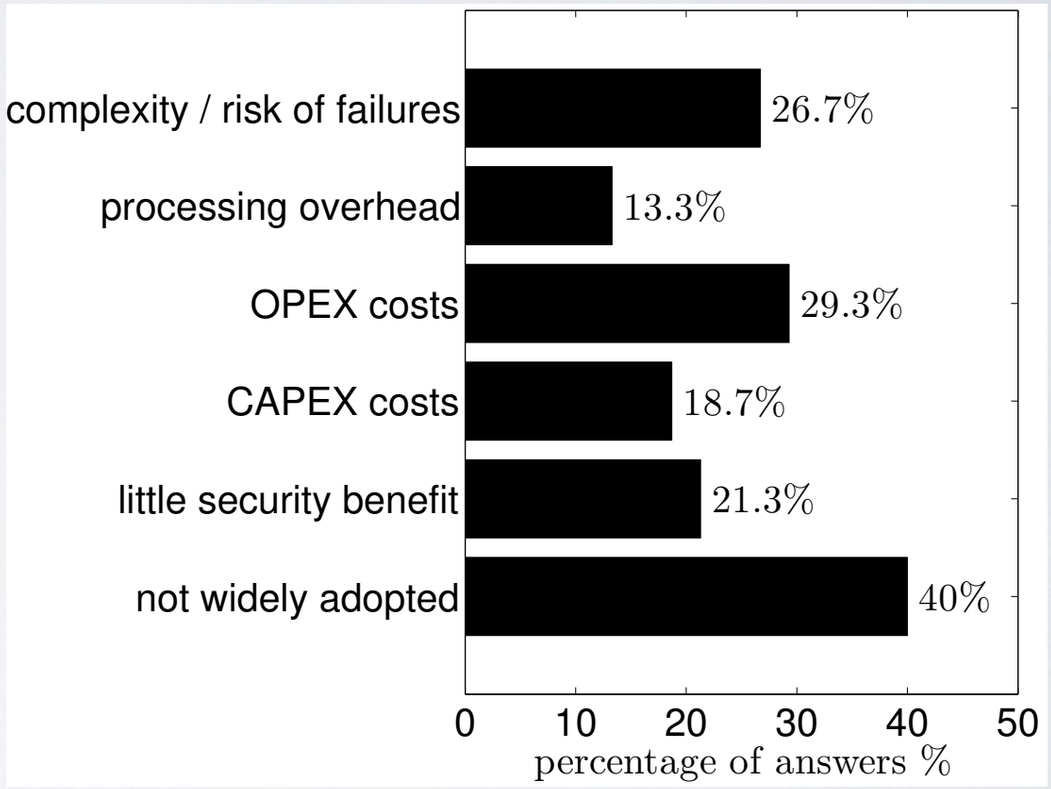
stealing/manipulating your routes



SOLUTIONS IN USE (1/2)

Proactive: RPKI

- Only 8% of prefixes covered by ROAs [1]
- Why? → limited adoption & costs/complexity [2]
- Does not protect the network against all attack types



Reasons for not using RPKI [2]

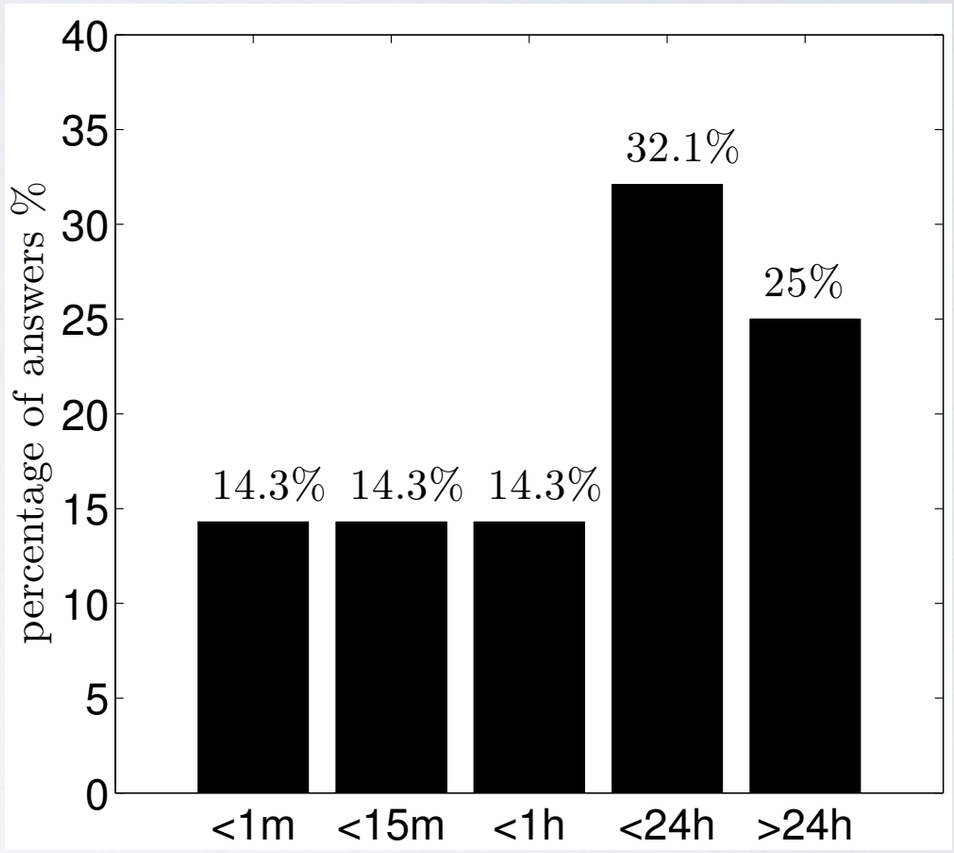
[1] NIST. RPKI Monitor https://rpki-monitor.antd.nist.gov/. May 2018

[2] P. Sermpezis, et. al., "A survey among Network Operators on BGP Prefix Hijacking", in ACM SIGCOMM CCR, Jan 2018.

SOLUTIONS IN USE (2/2)

Reactive: 3rd Party Services

- **Comprehensiveness**: detect only simple attacks
- **Accuracy**: prone to false positives (FP) & false negatives (FN)
- **Speed**: manual verification & then manual mitigation
- **Confidentiality**: need to share private info, routing policies, *etc.*



How much time an operational network was affected by a hijack [2]

[2] P. Sermpezis, et. al., "*A survey among Network Operators on BGP Prefix Hijacking*", in ACM SIGCOMM CCR, Jan 2018.

DETECTION BY 3RD PARTIES

...

3rd Party Detection

oAS
(your network)

BAD_AS

simple hijack

Polluted AS
(remote users)

ARTEMIS APPROACH

self-managed detection & mitigation

ARTEMIS

oAS
(your network)

BAD_AS

simple hijack

Polluted AS
(remote users)

A PARADIGM SHIFT

From 3rd party monitoring to Self-Operated

3rd Party

- **Evasion**
  - Detect only simple attacks
- **Accuracy**
  - Potential for lots of *FPs*
  - or alternatively lots of *FNs*
- **Speed**
  - Manual verification & then manual mitigation
- **Privacy**
  - Need to share private information

ARTEMIS

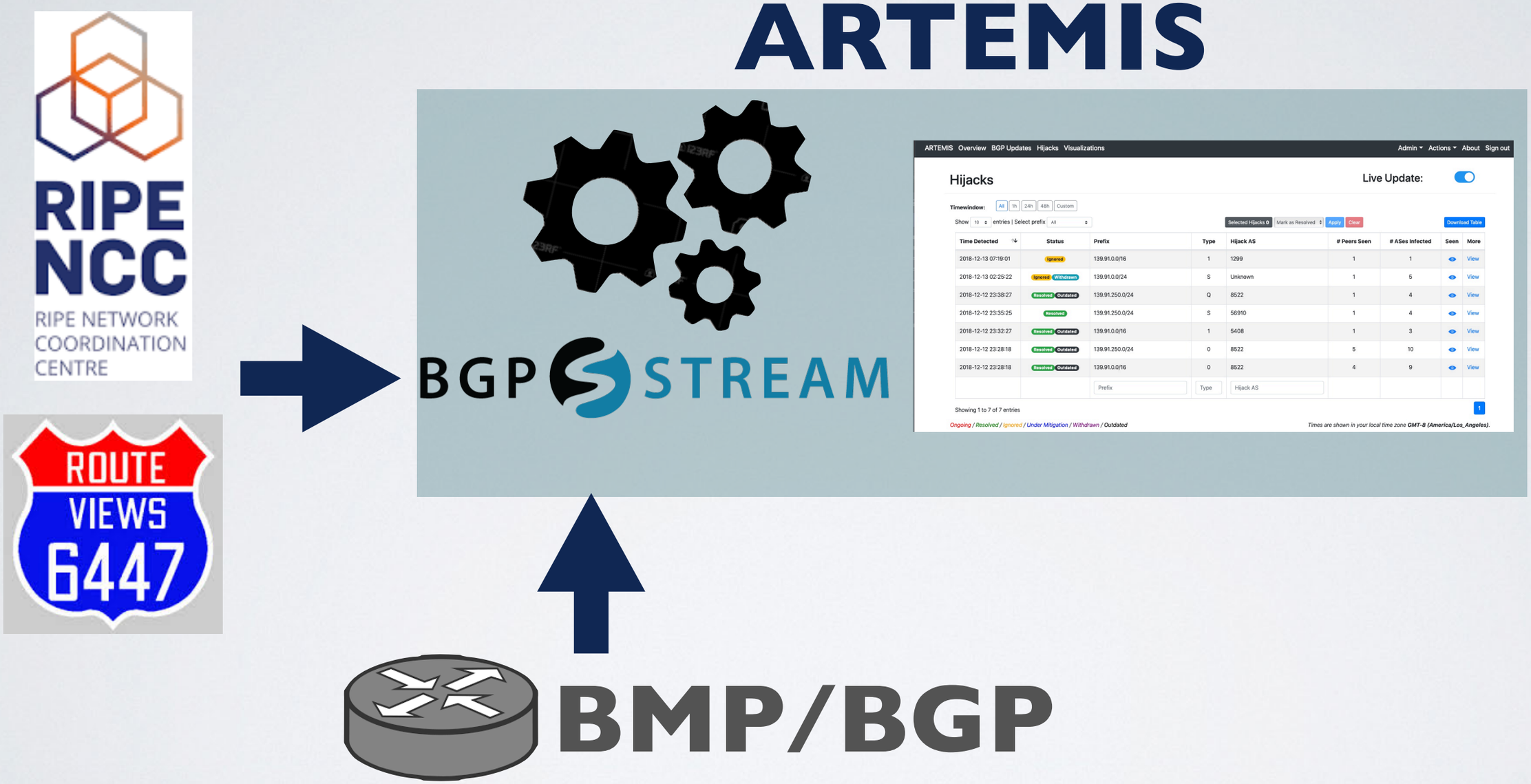
- **Evasion**
  - Covers *all* attack configurations
- **Accuracy**
  - *0% FP, 0% FN:* for most attacks
  - *0% FN* for the remaining ones (or manage *FP-FN* trade-off)
- **Speed**
  - Automated mitigation: neutralize attacks in a *minute*
- **Privacy & Flexibility**
  - *full privacy*

Sermpezis et al. , "ARTEMIS: Neutralizing BGP Hijacking within a Minute"
IEEE/ACM Transactions on Networking 2018

ARTEMIS

self-managed detection & mitigation

https://github.com/FORTH-ICS-INSPIRE/artemis



Sermpezis et al. , "ARTEMIS: Neutralizing BGP Hijacking within a Minute"
IEEE/ACM Transactions on Networking 2018

Center for Applied Internet Data Analysis
University of California San Diego

Foundation for Research and Technology-Hellas
University of Crete,
INSTITUTE OF COMPUTER SCIENCE

TEST DEPLOYMENT

https://github.com/FORTH-ICS-INSPIRE/artemis

merit
NETWORK. SECURITY. COMMUNITY.

GPN
GREAT PLAINS NETWORK
CONNECTING NETWORKS • ADVOCATING RESEARCH • CULTIVATING COMMUNITY
www.greatplains.net

COMCAST

INTERNET2®

NSF OAC-1848641 — Sep 2018 - Aug 2019
Experimental Deployment of the ARTEMIS BGP Hijacking Detection Prototype in Research and Educational Networks

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

Foundation for Research and Technology-Hellas
University of Crete,
FORTH
INSTITUTE OF COMPUTER SCIENCE

ARTEMIS DEMO

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

username: "guest" — password: "guest@artemis2018"

ARTEMIS Overview BGP Updates Hijacks Visualizations Admin Actions About Sign out

Hijacks

Live Update:

Timewindow: All 1h 24h 48h Custom

Show 10 entries | Select prefix All

Selected Hijacks 0 | Mark as Resolved | Apply | Clear | Download Table

Time Detected	Status	Prefix	Type	Hijack AS	# Peers Seen	# ASes Infected	Seen	More
2018-12-13 07:19:01	Ignored	139.91.0.0/16	1	1299	1	1		View
2018-12-13 02:25:22	Ignored Withdrawn	139.91.0.0/24	S	Unknown	1	5		View
2018-12-12 23:38:27	Resolved Outdated	139.91.250.0/24	Q	8522	1	4		View
2018-12-12 23:35:25	Resolved	139.91.250.0/24	S	56910	1	4		View
2018-12-12 23:32:27	Resolved Outdated	139.91.0.0/16	1	5408	1	3		View
2018-12-12 23:28:18	Resolved Outdated	139.91.250.0/24	0	8522	5	10		View
2018-12-12 23:28:18	Resolved Outdated	139.91.0.0/16	0	8522	4	9		View
		Prefix	Type	Hijack AS				

Showing 1 to 7 of 7 entries

1

Ongoing / Resolved / Ignored / Under Mitigation / Withdrawn / Outdated

*Times are shown in your local time zone **GMT-8 (America/Los_Angeles)**.*

THANKS

alberto@caida.org

Center for Applied Internet Data Analysis
University of California San Diego