Neutralizing BGP Hijacking within a Minute

-

Εξουδετέρωση επιθέσεων BGP στο λεπτό

(funded by RIPE NCC RIPE NETWORK COORDINATION CENTRE Community Projects 2017)

Vasileios Kotronis

(Joint work with: Pavlos Sermpezis, Petros Gigis, Dimitris Mavrommatis, Xenofontas Dimitropoulos, Alberto Dainotti, Alistair King)

GRNET Digital Technology Symposium, 6 November, 2018

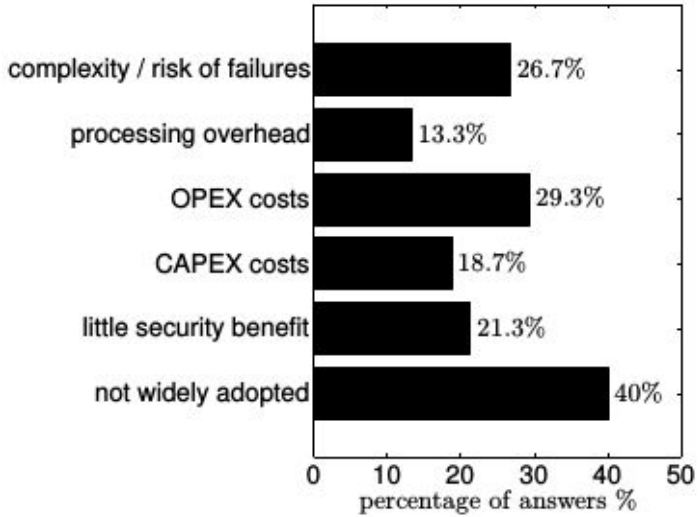
FORTH INSTITUTE OF COMPUTER SCIENCE

INternet Security & Privacy Intelligence REsearch Group

caida

How do people deal with hijacks today?→ **RPKI**

- X **< 10%** of prefixes covered by ROAs [1]
- X Why? → limited adoption & costs/complexity [2]
- X Does not protect the network against all attack types



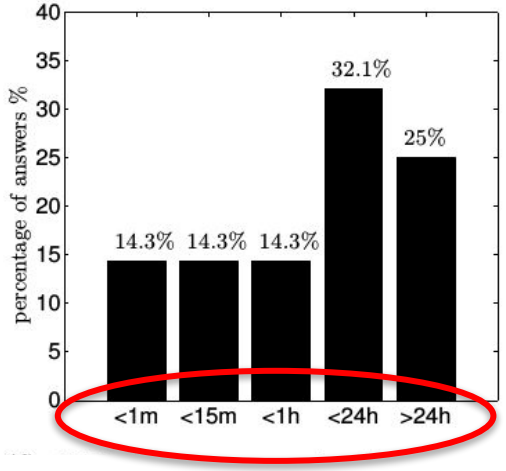
Reasons for not using RPKI [2]

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

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

How do people deal with hijacks today? → **3rd parties**

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



How much time an operational network was affected by a hijack [1]

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

Our solution: ARTEMIS

- Operated in-house: no third parties
- Real-time Detection
- Automatic Mitigation

✓ **Comprehensive**: covers *all* hijack types
✓ **Accurate**: *0% FP*, *0% FN* for basic types;
low tunable FP-FN trade-off for remaining types
✓ **Fast**: neutralizes (detect & mitigate) attacks in < *1 minute*
✓ **Privacy preserving**: no sensitive info shared
✓ **Flexible**: configurable mitigation per-prefix + per-hijack type

[1] ARTEMIS website www.inspire.edu.gr/artemis/
[2] P. Sermpezis et al., "ARTEMIS: Neutralizing BGP Hijacking within a Minute", in ACM/IEEE ToN, vol. 26, iss. 6, 2018.
[3] G. Chaviaras et al., "ARTEMIS: Real-Time Detection and Automatic Mitigation for BGP Prefix Hijacking", ACM SIGCOMM'16 demo.

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

BGP STREAM

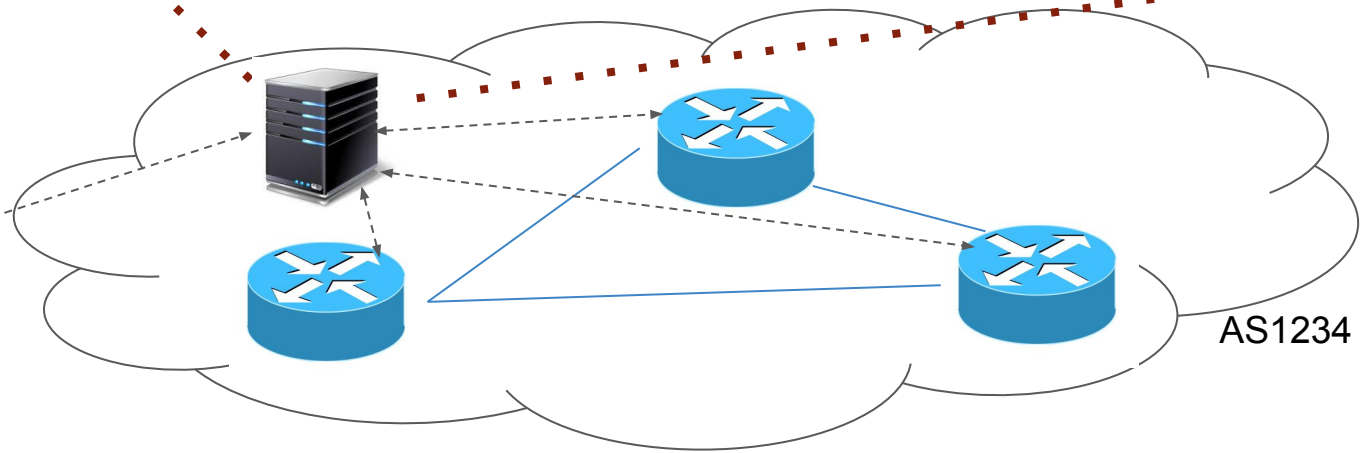
BGP Monitors:
- RIPE RIS
- BGPStream
  -- Live
  -- Historical
- Local (exaBGP)

Runs as a multi-container app in the NOC

ARTEMIS

MONITORING → DETECTION → MITIGATION

Operator Configuration File



AS1234

FORTH INSTITUTE OF COMPUTER SCIENCE

caida

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

BGP STREAM

BGP Monitors:
- RIPE RIS
- BGPStream
  -- Live
  -- Historical
- Local (exaBGP)

"Monitor X saw a BGP update for 10.0.0.0/23 originated by AS4."

"Origin sub-prefix HIJACK by AS4 vs. 10.0.0.0/23."

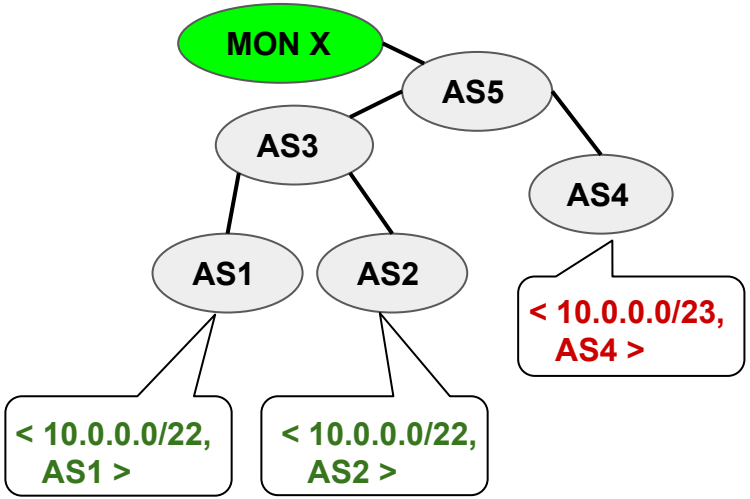
ARTEMIS

MONITORING → DETECTION → MITIGATION

React to hijack!

Operator Configuration File

"I own 10.0.0.0/22 and announce it from AS1 and AS2; both have AS3 as upstream."



FORTH INSTITUTE OF COMPUTER SCIENCE
caida

BGP Monitors:
- RIPE RIS
- BGPStream
  -- Live
  -- Historical
- Local (exaBGP)

"2 monitors saw in last 5 minutes < 10.0.0.0/22, AS1, AS2, AS4, … >"

"Link AS2-AS4 not seen in last 10 months for any prefix or direction. Path manipulation exact -prefix HIJACK by AS4 vs. 10.0.0.0/22."

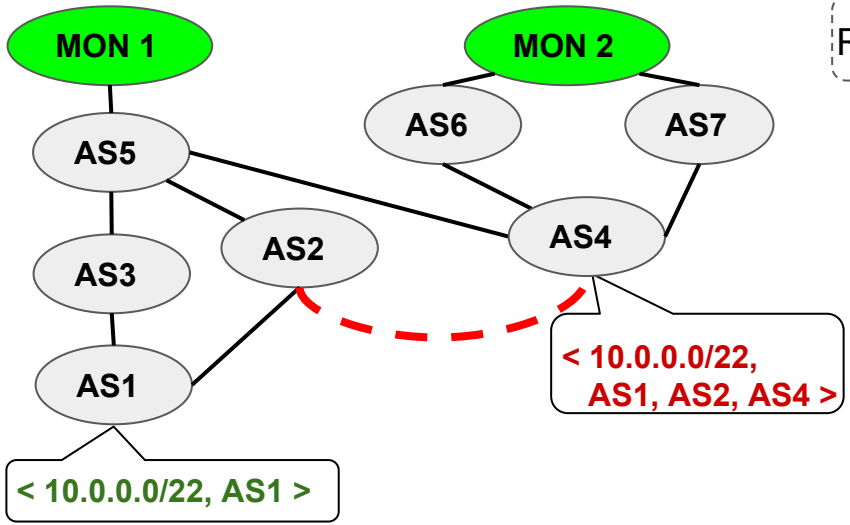
ARTEMIS

MONITORING → DETECTION → MITIGATION

React to hijack!

Operator Configuration File

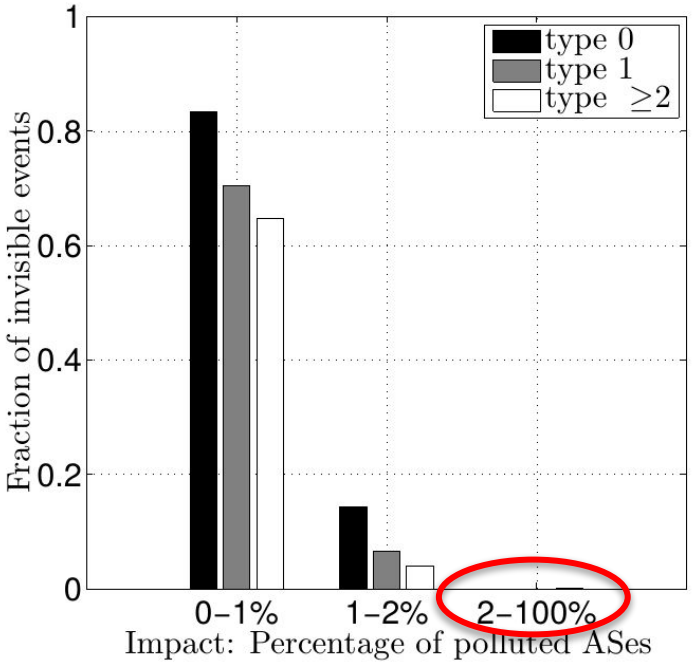
"I own 10.0.0.0/22 and announce it from AS1 with AS2 and AS3 as upstreams."



ARTEMIS: visibility of *all* impactful hijacks

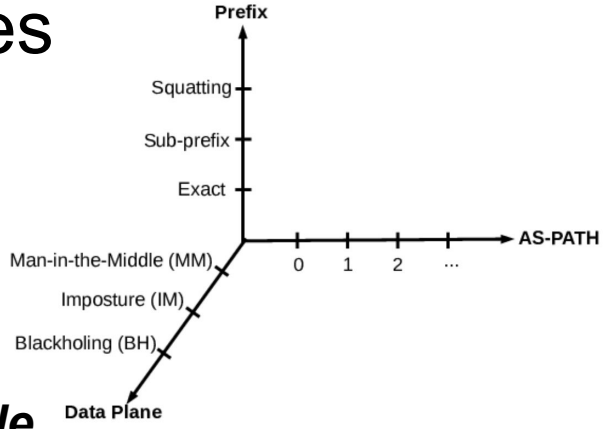
- Public BGP monitor infrastructure
  - RIPE RIS, RouteViews, BGPmon
  - ~500 vantage points worldwide (BGP routers)

Simulation results on the AS-level graph [1]



[1] P. Sermpezis et al., "*ARTEMIS: Neutralizing BGP Hijacking within a Minute*", in IEEE/ACM ToN, vol. 26, iss. 6, 2018.

ARTEMIS: detection of *all* hijack types



- Hijack types taxonomy - 3 dimensions:
  1. Affected prefixes:
     prefix or ***sub-prefix*** or ***squatting***
  2. Data-plane:
     blackholing or ***imposture*** or ***man-in-the-middle***
  3. AS-path manipulation: ***Type-0*** or ***Type-1*** or … or ***Type-N***
     - Legit announcement: <my_prefix, **MY_AS**>
     - Type-0 hijack: <my_prefix, **BAD_AS**, …>
     - Type-1 hijack: <my_prefix, **MY_AS**, **BAD_AS**, …>
     - Type-2 hijack: <my_prefix, **MY_AS**, MY_PEER, **BAD_AS**, …>
     - …
     - Type-N hijack: <my_prefix, **MY_AS**, ..., **BAD_AS**, …>
     - Type-U hijack: <my_prefix, unaltered_path>

FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS: detection of *all* hijack types

TABLE 1: Comparison of BGP prefix hijacking detection systems/services w.r.t. ability to detect different classes of attacks.

Class of Hijacking Attack			Control-plane System/Service			Data-plane System/Service		Hybrid System/Service		
Affected prefix	AS-PATH (Type)	Data plane	ARTEMIS	Cyclops (2008) [21]	PHAS (2006) [36]	iSpy (2008) [68]	Zheng *et al.* (2007) [70]	HEAP (2016) [57]	Argus (2012) [60]	Hu *et al.* (2007) [32]
Sub	U	*	✓	×	×	×	×	×	×	×
Sub	0/1	BH	✓	×	✓	×	×	✓	✓	✓
Sub	0/1	IM	✓	×	✓	×	×	✓	×	✓
Sub	0/1	MM	✓	×	✓	×	×	×	×	×
Sub	≥ 2	BH	✓	×	×	×	×	✓	✓	✓
Sub	≥ 2	IM	✓	×	×	×	×	✓	×	✓
Sub	≥ 2	MM	✓	×	×	×	×	×	×	×
Exact	0/1	BH	✓	✓	✓	✓	×	×	✓	✓
Exact	0/1	IM	✓	✓	✓	×	✓	×	×	✓
Exact	0/1	MM	✓	✓	✓	×	✓	×	×	×
Exact	≥ 2	BH	✓	×	×	✓	×	×	✓	✓
Exact	≥ 2	IM	✓	×	×	×	✓	×	×	✓
Exact	≥ 2	MM	✓	×	×	×	✓	×	×	×

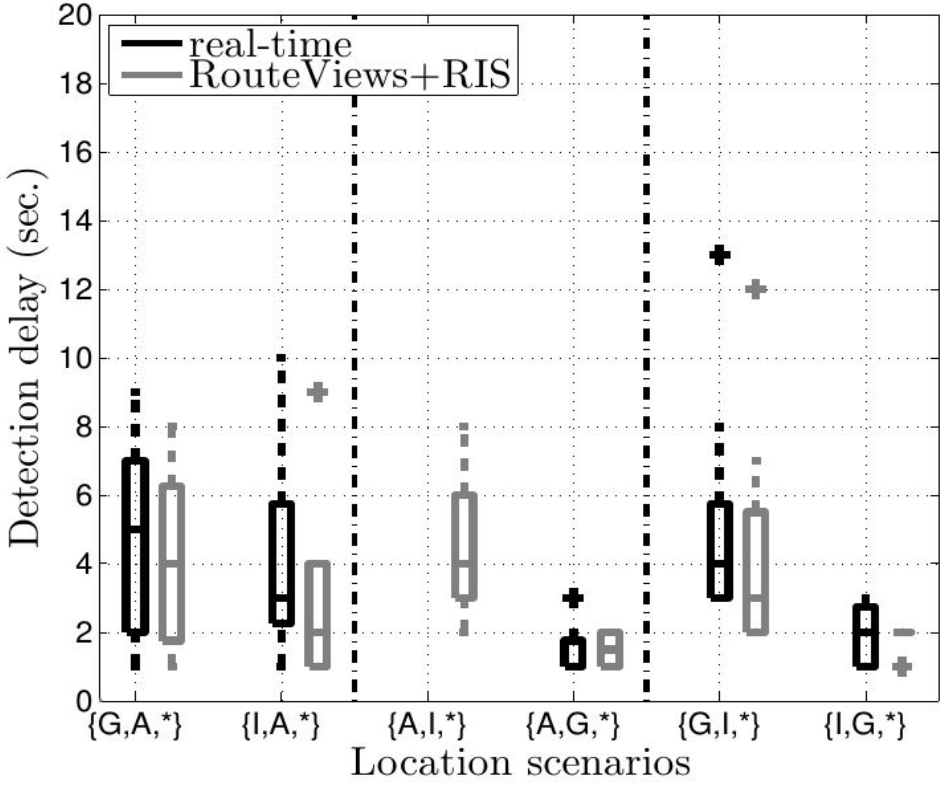
FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS: *accurate* detection

Hijacking Attack			ARTEMIS Detection				
Prefix	AS-PATH (Type)	Data Plane	False Positives (FP)	False Negatives (FN)	Detection Rule	Needed Local Information	Detection Approach
Sub-prefix	*	*	None	None	Config. vs BGP updates	Pfx.	Sec. 5.2
Squatting	*	*	None	None	Config. vs BGP updates	Pfx.	Sec. 5.2
Exact	0/1	*	None	None	Config. vs BGP updates	Pfx. + ASN (+ neighbor ASN)	Sec. 5.3
Exact	≥ 2	*	< 0.3/day for $> 73\%$ of ASes	None	Past Data vs BGP updates (bidirectional link)	Pfx.+ Past AS links	Sec. 5.4 *Stage 1*
Exact	≥ 2	*	None for 63% of ASes ($T_{s2} = 5min$, $th_{s2} > 1$ monitors)	$< 4\%$	BGP updates (waiting interval, bidirectional link)	Pfx.	Sec. 5.4 *Stage 2*

ARTEMIS: real-time monitoring, detection in *5 sec.*!

Real experiments in the Internet [1] (PEERING testbed)



[1] P. Sermpezis et al., "*ARTEMIS: Neutralizing BGP Hijacking within a Minute*", in IEEE/ACM ToN, vol. 26, iss. 6, 2018.

ARTEMIS: mitigation methods

- DIY: react by **de-aggregating** if you can
- Otherwise (e.g., /24 prefixes) **get help** from other ASes

  → *announcement (MOAS) and tunneling from siblings or helper AS(es)*

TABLE 7: Mean percentage of polluted ASes, when outsourcing BGP announcements to organizations providing DDoS protection services; these organizations can provide highly effective outsourced mitigation of BGP hijacking.

	without outsourcing	top ISPs	AK	CF	VE	IN	NE
Type0	50.0%	12.4%	2.4%	4.8%	5.0%	7.3%	11.0%
Type1	28.6%	8.2%	0.3%	0.8%	0.9%	2.3%	3.3%
Type2	16.9%	6.2%	0.2%	0.4%	0.4%	1.3%	1.1%
Type3	11.6%	4.5%	0.1%	0.4%	0.3%	1.1%	0.5%

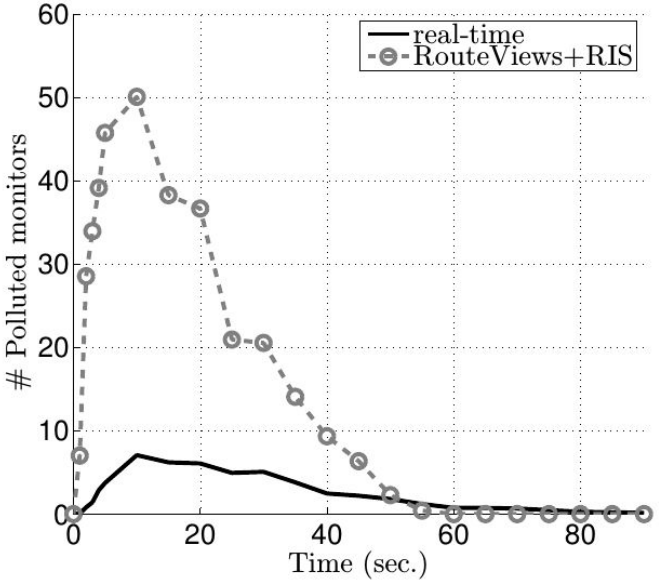
FORTH INSTITUTE OF COMPUTER SCIENCE caida

ARTEMIS: automated & flexible mitigation

- Automated: triggered immediately upon detection
- Flexible: configure per prefix / hijack type / impact / etc.

detection + mitigation:

NOW	ARTEMIS
hours/days →	**1 min.**



FORTH INSTITUTE OF COMPUTER SCIENCE caida

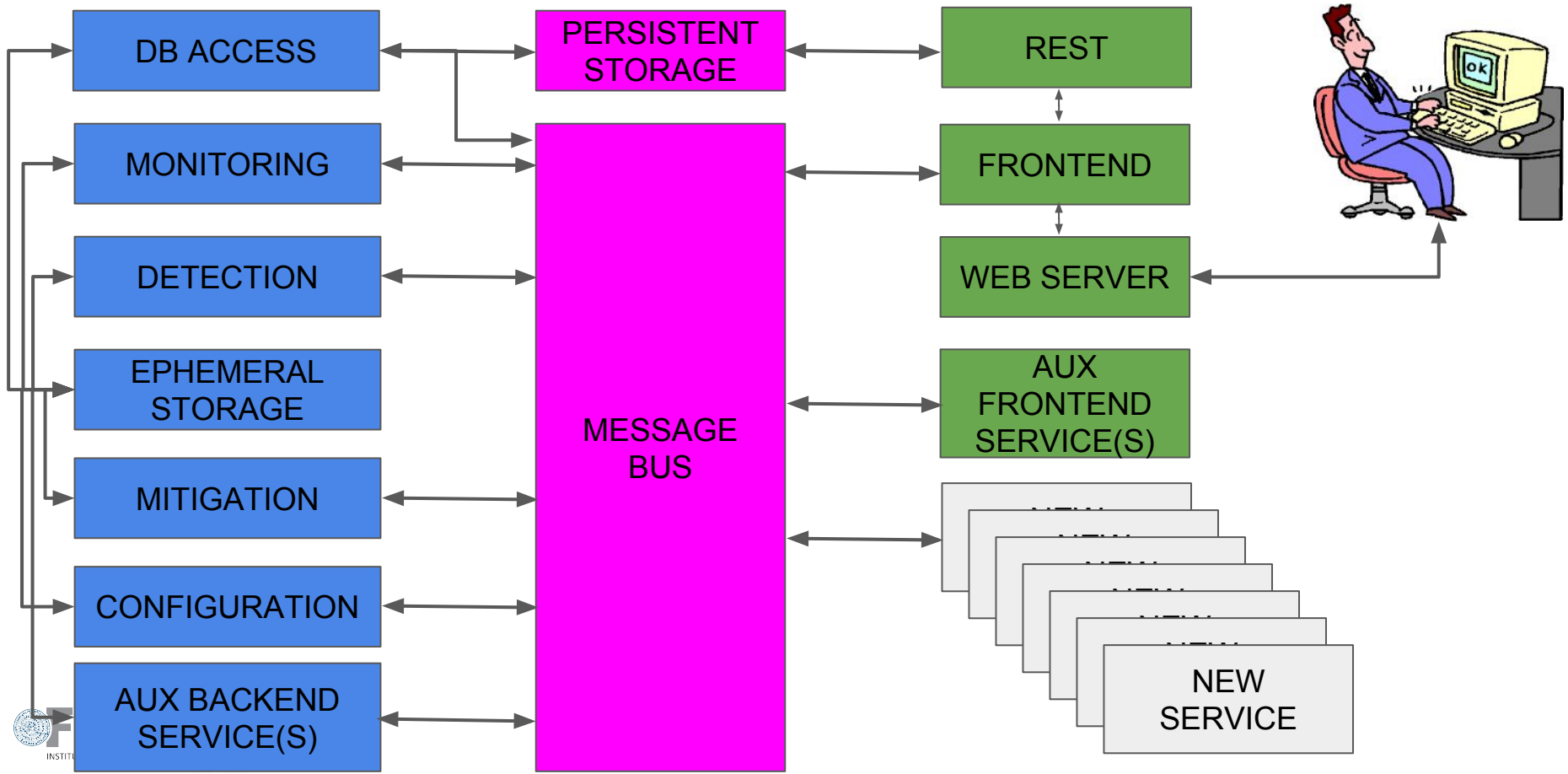
Prototype: supported features

- Real-time monitoring of BGP updates related to network's prefixes
- Real-time detection of BGP prefix hijacking attacks/events:
  - exact-prefix type-0/1
  - sub-prefix (of any type)
  - squatting attacks
- Syslog/email notifications of hijacks
- Manual mitigation of BGP prefix hijacking attacks
- Web interface used by the network administrator
- Support for both IPv4 and IPv6 prefixes
- Modularity/extensibility

Affected prefix	AS-PATH (Type)	Data plane	ARTEMIS
Sub	U	*	✓
Sub	0/1	BH	✓
Sub	0/1	IM	✓
Sub	0/1	MM	✓
Sub	≥ 2	BH	✓
Sub	≥ 2	IM	✓
Sub	≥ 2	MM	✓
Exact	0/1	BH	✓
Exact	0/1	IM	✓
Exact	0/1	MM	✓
Exact	≥ 2	BH	✓
Exact	≥ 2	IM	✓
Exact	≥ 2	MM	✓

FORTH INSTITUTE OF COMPUTER SCIENCE caida

Prototype: High-level system overview



Prototype: configuration file

- Define prefix, ASN, monitor groups
- Declare ARTEMIS rules:
  - “My ASes ASX and ASY originate prefix P”
  - “And they advertise it to ASZ”
  - “When a hijack occurs → mitigate manually”

Sample Rule	Sample Incoming BGP update	Hijack
prefixes: - *my_prefix origin_asns: - *my_origin neighbors: - *my_neighbor mitigation: manual	[..., <subprefix_of_my_prefix>]	S
	[..., <not_my_origin>, <my_prefix>]	0
	[..., <not_my_neighbor>, <my_origin>, <my_prefix>]	1
prefixes: - *my_prefix mitigation: manual	[..., <my_prefix>]	Q

```
#
# ARTEMIS Configuration File
#
# Start of Prefix Definitions
prefixes:
          forth_prefix_main: &forth_prefix_main
          - 139.91.0.0/16
          forth_prefix_lamda: &forth_prefix_lamda
          - 139.91.250.0/24
          forth_prefix_vod: &forth_prefix_vod
          - 139.91.2.0/24
# End of Prefix Definitions
# Start of Monitor Definitions
monitors:
          riperis: ['']
          bgpstreamlive:
          - routeviews
          - ris
          betabmp:
          - betabmp
          # exabgp:
          # - ip: 192.168.1.1
          #   port: 5000
# End of Monitor Definitions
# Start of ASN Definitions
asns:
          forth_asn: &forth_asn
          8522
          grnet_forth_upstream: &grnet_forth_upstream
          5408
          lamda_forth_upstream_back: &lamda_forth_upstream_back
          56910
          vodafone_forth_upstream_back:
&vodafone_forth_upstream_back
          12361
# End of ASN Definitions
# Start of Rule Definitions
rules:
```

Prototype: What's next?

- Open-sourcing ARTEMIS
- Revamped UI
- Monitoring hijack progress automatically
- Automated configuration
- Advanced detection + mitigation
- Using data-plane measurements for
  - automated verification of hijack events
  - detection of events with limited regional impact
- Cooperation with CAIDA on Internet Observatory
  - centralized service for detection of BGP hijacks and anomalies (including MitM)

Thank you!

- Current ARTEMIS testers:
  - Major greek ISP
  - Internet2 (major US academic network)
  - FORTH (dual-homed edge network)
- What do we want from you?
  - Feedback
  - Advice on integrating ARTEMIS in operational environments
  - Collaboration for testing ARTEMIS (e.g., configuration)
  - Try demo at: http://inspire.edu.gr/artemis/demo/ (creds: guest / guest@artemis2018)
  - Mail me at: *vkotronis@ics.forth.gr*
  - Visit the ARTEMIS website *http://www.inspire.edu.gr/artemis/*

FORTH INSTITUTE OF COMPUTER SCIENCE
caida
INternet Security & Privacy Intelligence REsearch Group

funded by: RIPE NCC RIPE NETWORK COORDINATION CENTRE
NSF
erc European Research Council Established by the European Commission
EU338402

BACKUP

BGP prefix hijacking is a critical threat

→ to your **organization** & **customers** & **peers**

BACKUP

- **Outages** in the Internet cause losses of millions of $$$
- **Interception** of bitcoins, credit card transactions, passwords, ...
- **Bad reputation** for hijacked networks: security, service reliability

...only in 2017: ***5,304*** hijacks, with ***3,106*** organizations as victims [1]

[1] “14,000 Incidents: A 2017 Routing Security Year in Review”, www.internetsociety.org

Threat Model → the hijacker:

- controls a single AS and its edge routers
- has full control of the control plane and data plane within its own AS
- can arbitrarily manipulate the:
  - BGP messages that it sends to its neighboring ASes (control plane)
  - traffic that crosses its network (data plane)
- has otherwise no control over BGP messages and traffic exchanged between two other ASes.

BACKUP

→ Extensions (future work): multiple ASes controlled by a single hijacker

Type-N, N≥2, hijacks: Stage 1

BACKUP

- Triggered upon a BGP update (for a monitored prefix) whose AS-PATH contains a N-hop AS-link (N ≥ 2) that is not included in the previously verified AS-links list
- Legitimate if this link has been observed in the opposite direction in the AS-links list from monitors and local BGP routers
  (10 months history) (and there appears consistently at least 1 AS on the left of the link*)
- Example with fake link directly attached to hijacker:

<my_prefix, **MY_AS**, MY_PEER, **BAD_AS**, …> attack announcement

<any_prefix, ..., **BAD_AS**, MY_PEER, …, **BAD_AS**, ...> pre-attack fails (discard loops)

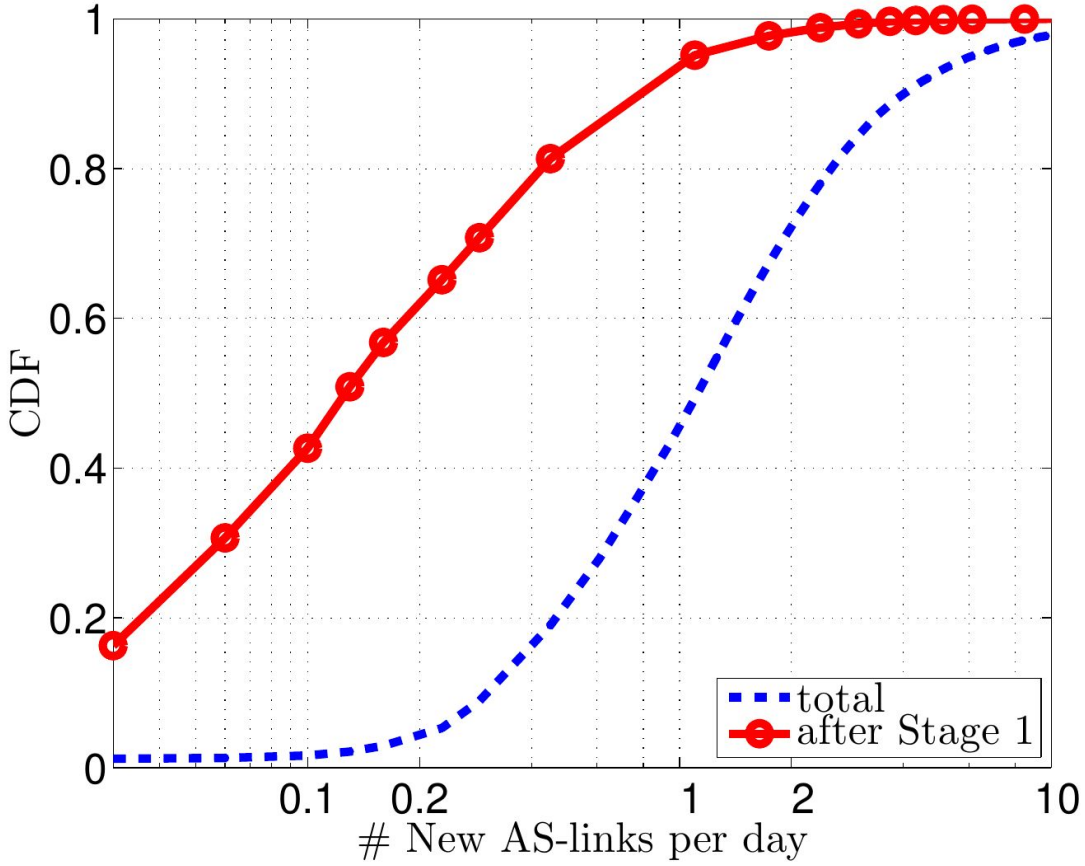
<any_prefix, ..., **BAD_AS**, MY_PEER, …, **2nd_BAD_AS**, ...> pre-attack succeeds
(beyond adopted threat model)

- * Works also when hijacker is hiding behind a legitimate upstream provider!

FORTH INSTITUTE OF COMPUTER SCIENCE caida

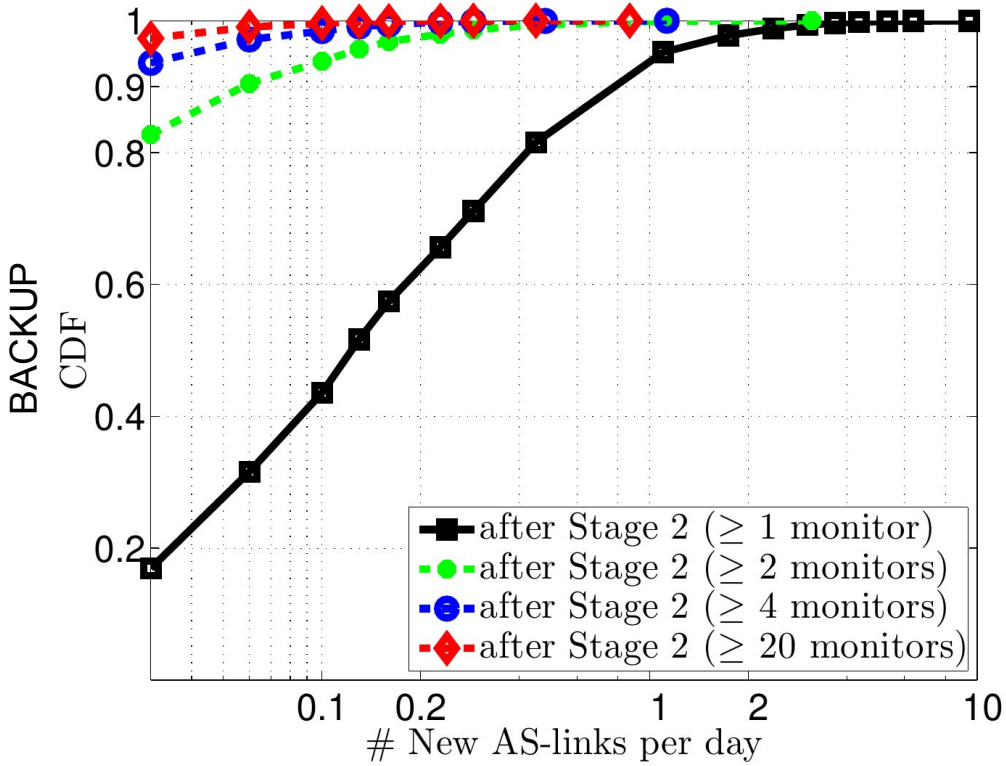
Type-N, N≥2, hijacks: Stage 1

BACKUP



FORTH INSTITUTE OF COMPUTER SCIENCE caida

Type-N, N≥2, hijacks: Stage 2 w/ FN of small impact



- **Stage 2**
  - Wait 5 minutes
  - Recheck tables on monitors + local routers
  - Optional: decisions based on observable impact (e.g., number of monitors involved)

FORTH INSTITUTE OF COMPUTER SCIENCE caida

Note: What we do not cover as hijacks →route leaks

- Not actual hijacks in the classic threat model
  - All links involved in the announced paths are valid!
- Fall in the context of “policy violations”, e.g.,
  - What if Google decided to be a Tier-1 global transit network for one hour?
  - What if your friendly IXP peer decided to act as your upstream?
- Detecting them requires detailed knowledge of in-path policies
  - These are not publicly available
  - Existing datasets → would yield high numbers of FP
  - 30% of observed routes are not consistent with available routing policy data [1]
  - **Ongoing work! (beyond “good filtering”)**

BACKUP

[1] Ruwaifa Anwar et al. Investigating interdomain routing policies in the wild. In Proc. ACM IMC, 2015.