PANDA with Augmented IP Level Data

Yves Vanaubel, Benoit Donnet

AIMS Workshop, March 2018

mami
measurement and architecture for a middleboxed internet

LIÈGE université

measurement | architecture | experimentation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.The opinions expressed and arguments employed reflect only the authors' view. The European Commission is not responsible for any use that may be made of that information.

Agenda

- PANDA with MPLS
- PANDA with Middleboxes
- PANDA with improved alias resolution
- Conclusion

PANDA with MPLS

- MPLS tunnels might be hidden or not to `traceroute` exploration
  - B. Donnet, M. Luckie, P. Mérindol, J.-J. Pansiot. *Revealing MPLS Tunnels Obscured from Traceroute*. In ACM SIGCOMM Computer Communication Review. 42(2). pg. 87-93. April 2012.
- In case of content hidden to `traceroute`
  - artificial high degree node
  - artificial high delay
  - false links between nodes
  - Y. Vanaubel, P. Mérindol, J.-J. Pansiot, B. Donnet. *Through the Wormhole: Tracking Invisible MPLS Tunnels*. In Proc. ACM Internet Measurement Conference (IMC). November 2017.

PANDA with MPLS (2)

- In case of "truly" invisible tunnels
  - tunnel content does not appear in `traceroute` output
  - MPLS labels are not included in the `time exceeded` messages
- We need triggers to infer their presence
  - Y. Vanaubel, P. Mérindol, J.-J. Pansiot, B. Donnet. *Through the Wormhole: Tracking Invisible MPLS Tunnels*. In Proc. ACM Internet Measurement Conference (IMC). November 2017.

PANDA with MPLS (3)

- The MPLS behavior is also related to the hardware brand
- Might be inferred through network fingerprinting
  - Y. Vanaubel, J-J. Pansiot, P. Mérindol, B. Donnet. *Network Fingerprinting: TTL-Based Router Signatures.* In Proc. ACM Internet Measurement Conference (IMC). November 2013
- Fingerprinting is based on initial TTL (iTTL) value when forging packet
  - should be set to 64 ([RFC1700])
  - in practice, iTTL may depend on
    - ✓ hardware (CISCO vs. Juniper)
    - ✓ operating system (JunOS vs. JunOSE vs. IOS vs. ...)
    - ✓ protocol (ICMP vs. UDP vs. TCP)
    - ✓ type of message (`time_exceeded` vs. `echo_reply` vs `destination_unreachable` vs. ...)

PANDA with MPLS (4)

- Signatures for major manufacturers

Manufacturer	<TE, ER>
Cisco	**<255, 255>**
Juniper (JunOS)	**<255, 64>**
Juniper (JunOSE)	**<128, 128>**
Brocade, Alcatel, and Linux Boxes	**<64, 64>**

PANDA with MPLS (5)

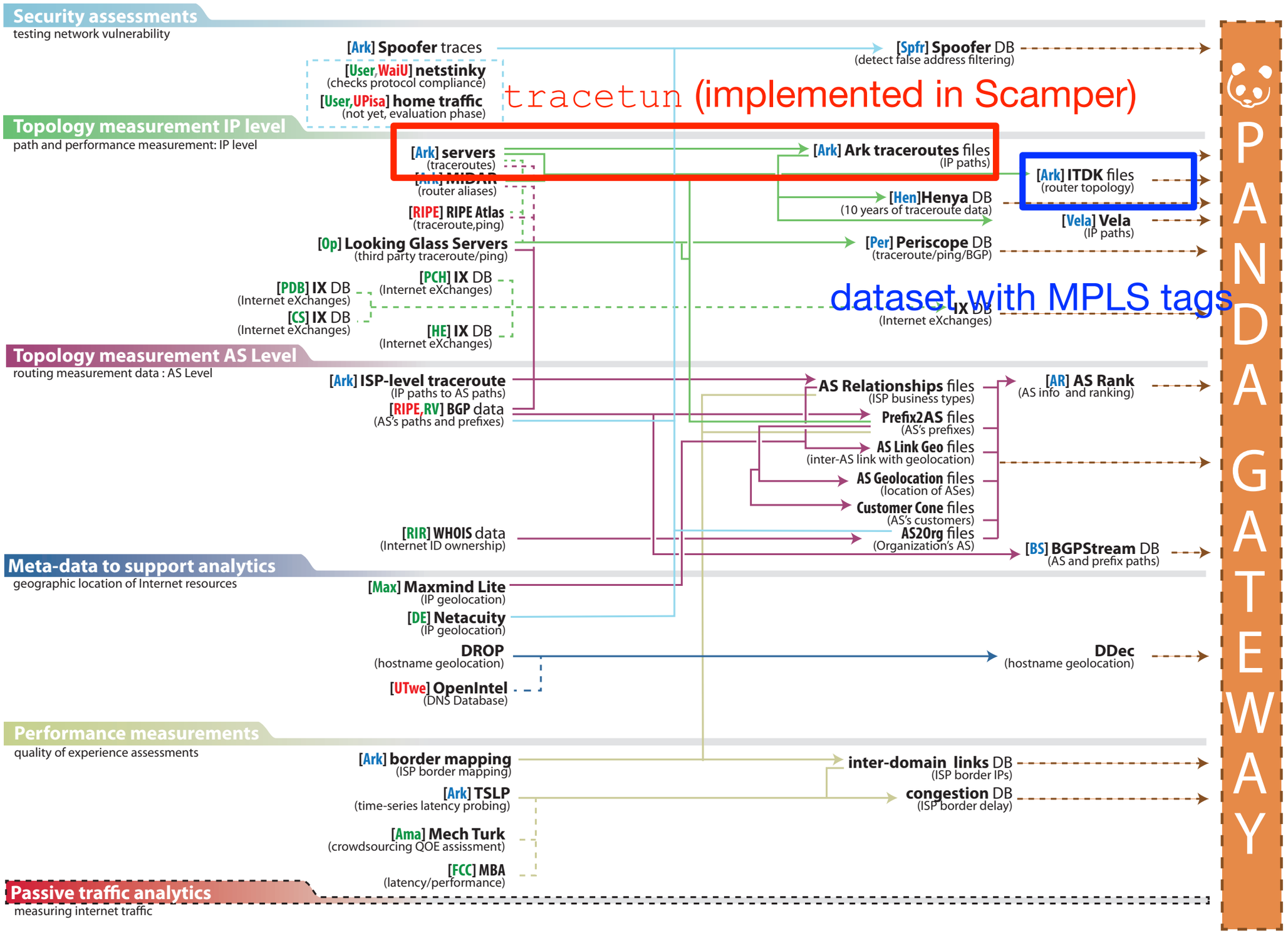
- Update: 99% of tunnels can now be revealed

	RFC4950		no RFC4950	
	Explicit		**Implicit**	
ttl_propagate	**Signature** <255,255> <255,64> <255,*> …	**MPLS Indication** LSE	**Signature** <64,64> <255,*> <255,64>	**MPLS Revelation** qTTL UTURN
	Opaque		**Invisible**	
no_ttl_propagate	**Signature** <255,255>	**Triggers** LSE LSE-TTL	**IP Revelation** DPR BRPR	

Pop	**Signature**	**Triggers**	**IP Revelation**
UHP	<255,255>	DUPLICATE_IP	DPR, BRPR
PHP	<255,64> <255,*> <255,255>	RTLA FRPLA	DPR BRPR
Hybrid (UHP/PHP)	<255,255>		DPR BRPR

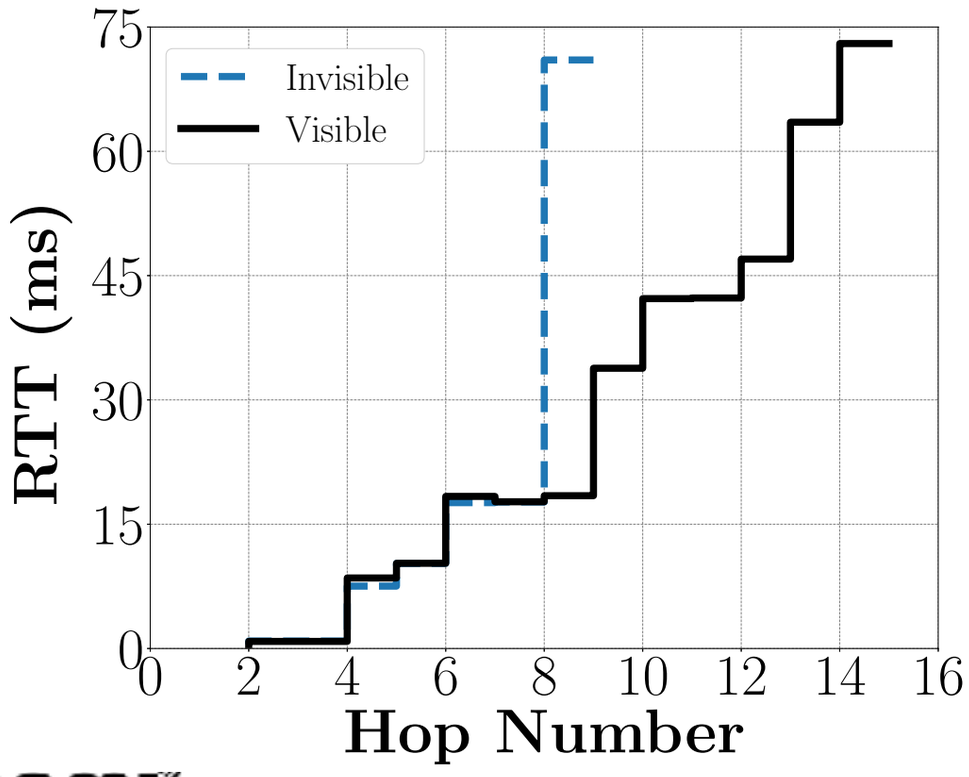
Can't be revealed at a reasonable cost

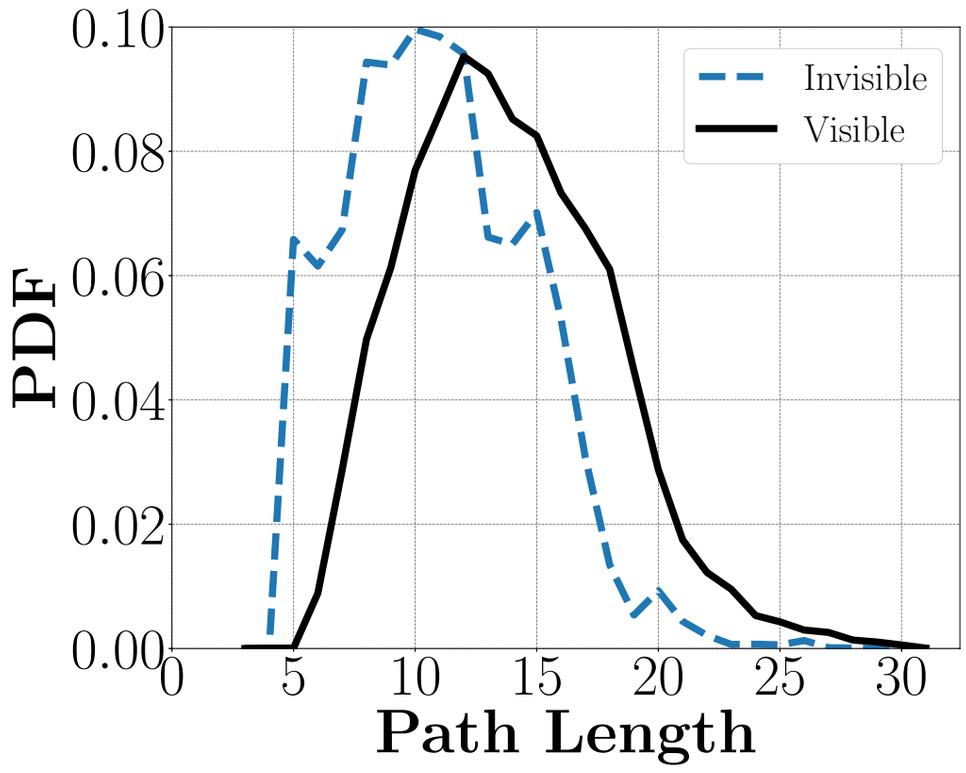
PANDA with MPLS (6)



PANDA with MPLS (7)

- Expected analysis through PANDA gateway
  - Traffic Engineering analysis
    - ✓ Y. Vanaubel, P. Mérindol, J.-J. Pansiot, B. Donnet. *MPLS under the Microscope: Revealing Actual Transit Path Diversity*. In Proc. ACM Internet Measurement Conference (IMC). October 2015
  - RTT correction
  - graph properties correction





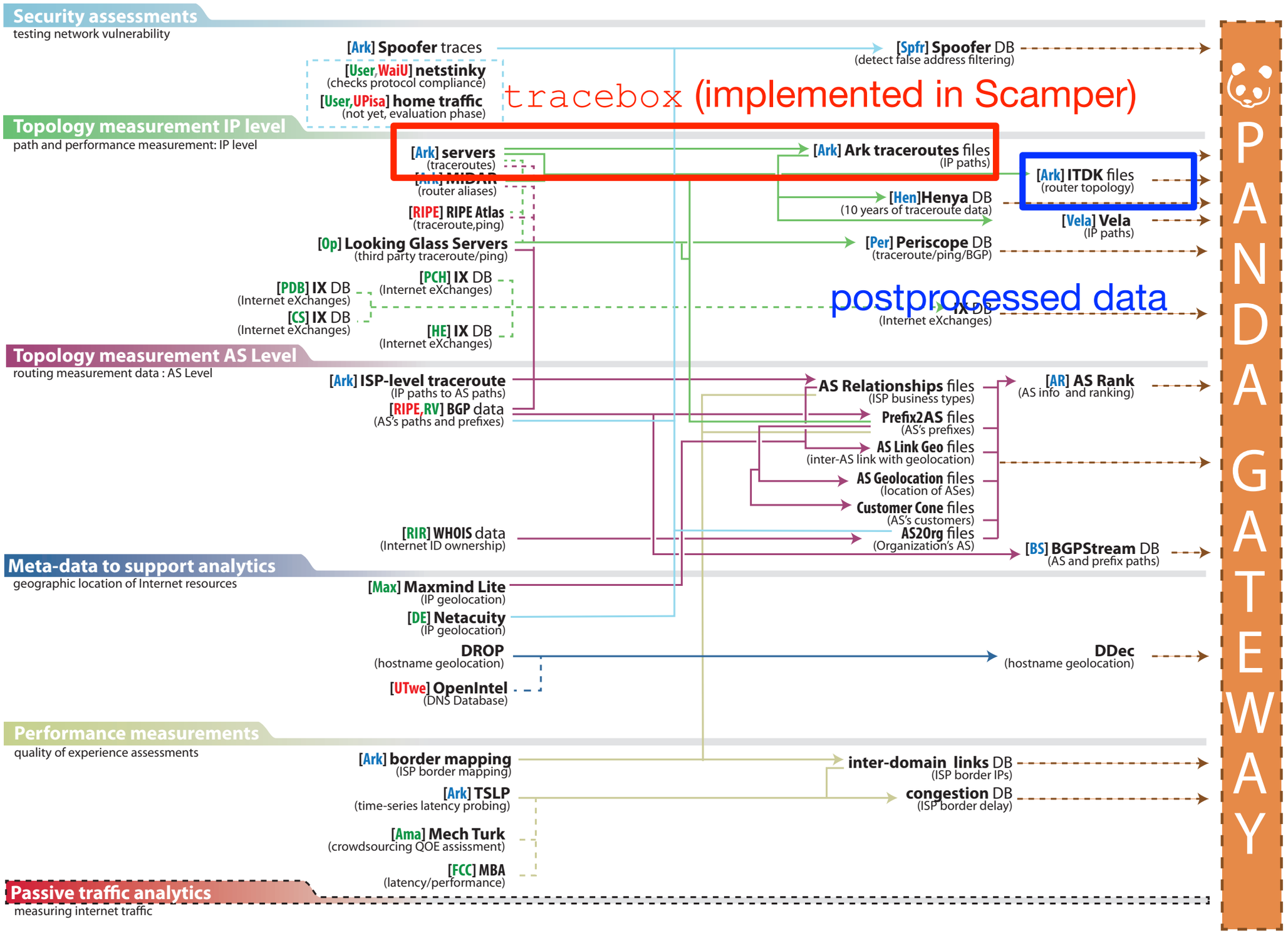
PANDA with Middleboxes

- `tracebox` is an extension to `traceroute`
  - send TTL limited probes
  - inspect incoming ICMP time_exceeded packets
    - ✓ compare the TCP probe quoted and the TCP probe sent
    - ✓ in case of difference(s), a middlebox is found along the path
  - already implemented in Scamper
    - ✓ see https://github.com/mami-project/tracebox
  - G. Detal, B. Hesmans, O. Bonaventure, Y. Vanaubel, B. Donnet. *Revealing Middlebox Interference with Tracebox*. In Proc. ACM Internet Measurement Conference (IMC). October 2013.

PANDA with Middleboxes (2)

- Extensions to tracebox for supporting large-scale dataset
  - offline analysis
  - K. Edeline, B. Donnet. *A First Look at the Prevalence and Persistence of Middleboxes in the Wild*. In Proc. International Teletraffic Congress (ITC). September 2017.

PANDA with Middleboxes (3)



PANDA with Middleboxes (4)

- PANDA gateway might be "merged" with (or linked to) the *Path Transparency Observatory* (PTO)
  - see https://observatory.mami-project.eu
  - gives information on path transparency and middleboxes interference

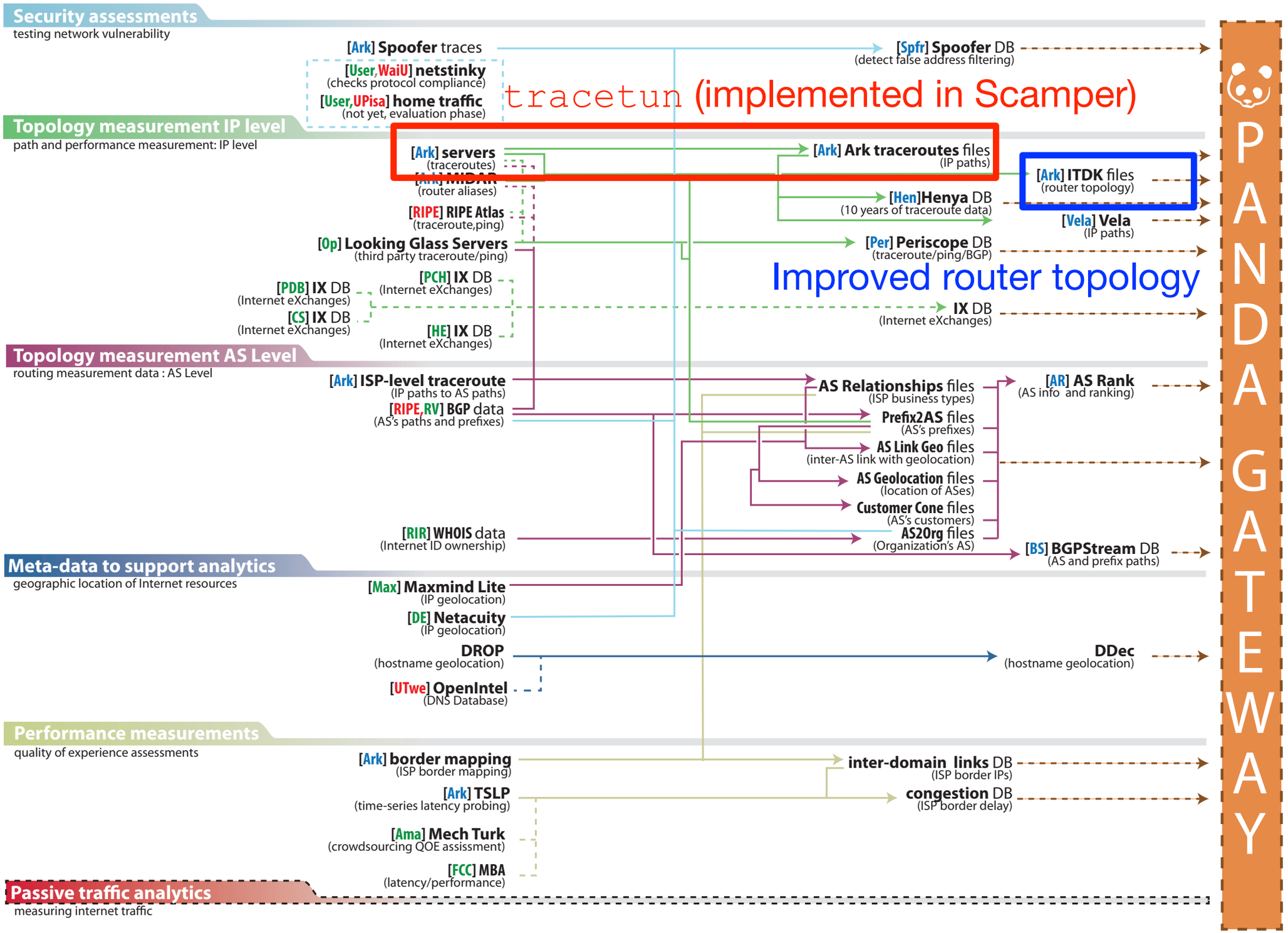
PANDA with Middleboxes (5)

- Expected analysis through the PANDA portal
  - Improved vision of the topology
    - ✓ middleboxes are a large part of the network
    - ✓ better AS "anatomy"
  - Path transparency

PANDA with Improved Alias Resolution

- Fingerprinting might be used for alias resolution
  - 2 IP interfaces with different fingerprints cannot be aliases
- Fingerprinting already implemented in
  - `tracetun`
  - in Scamper, as an independent module
    - ✓ see https://github.com/fhoe/networkFingerprinting
- Expected results
  - speed up alias resolution
  - improve accuracy
  - J.-F. Grailet, B. Donnet. *Towards a Renewed Alias Resolution with Space Search Reduction and IP Fingerprinting*. In Proc. Network Traffic Measurement and Analysis Conference (TMA). June 2017

PANDA with Improved Alias Resolution (2)



Conclusion

- Improving the PANDA architecture with
  - additional probing techniques
    - ✓ MPLS detection
    - ✓ middleboxes
    - ✓ fingerprinting
  - more complete dataset
- ... should lead to more complete data analysis on the PANDA portal, e.g.,
  - AS anatomy
    - ✓ MPLS, middleboxes usage, ...
  - path transparency
  - topology modeling