

PANDA with Augmented IP Level Data

Yves Vanaubel, Benoit Donnet

AIMS Workshop, March 2018



measurement and architecture for a middleboxed internet



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	MPLS Indication			Signature	MPLS Revelation	
	<255,255> <255,64> <255,*> ...	LSE			<64,64> <255,*> <255,64>	qTTL UTURN	
no_ttl_propagate	Opaque			Invisible			
	Signature	Triggers	IP Revelation	Pop	Signature	Triggers	IP Revelation
	<255,255>	LSE LSE-TTL	DPR BRPR	UHP	<255,255>	DUPLICATE_IP	DPR, BRPR
				PHP	<255,64> <255,*> <255,255>	RTL FRPLA	DPR BRPR
			Hybrid (UHP/PHP)	<255,255>		DPR BRPR	

Can't be revealed at a reasonable cost

PANDA with MPLS (6)



P
A
N
D
A
G
A
T
E
W
A
Y

Security assessments

testing network vulnerability

[Ark] Spoofer traces
[User,WaiU] netstinky (checks protocol compliance)
[User,UPisa] home traffic (not yet, evaluation phase)

[Spfr] Spoofer DB (detect false address filtering)

tracetun (implemented in Scamper)

Topology measurement IP level

path and performance measurement: IP level

[Ark] servers (traceroutes)
[MIPAR] MIPAR (router aliases)
[RIPE] RIPE Atlas (traceroute,ping)
[Op] Looking Glass Servers (third party traceroute/ping)
[PDB] IX DB (Internet eXchanges)
[CS] IX DB (Internet eXchanges)
[PCH] IX DB (Internet eXchanges)
[HE] IX DB (Internet eXchanges)

[Ark] Ark traceroutes files (IP paths)

[Ark] ITDK files (router topology)

[Hen] Henya DB (10 years of traceroute data)

[Vela] Vela (IP paths)

dataset with MPLS tags

[Per] Periscope DB (traceroute/ping/BGP)

[IX] IX DB (Internet eXchanges)

Topology measurement AS Level

routing measurement data : AS Level

[Ark] ISP-level traceroute (IP paths to AS paths)
[RIPE,RV] BGP data (AS's paths and prefixes)

AS Relationships files (ISP business types)

[AR] AS Rank (AS info and ranking)

Prefix2AS files (AS's prefixes)

AS Link Geo files (inter-AS link with geolocation)

AS Geolocation files (location of ASes)

Customer Cone files (AS's customers)

AS2Org files (Organization's AS)

[BS] BGPStream DB (AS and prefix paths)

[RIR] WHOIS data (Internet ID ownership)

Meta-data to support analytics

geographic location of Internet resources

[Max] Maxmind Lite (IP geolocation)

[DE] Netacuity (IP geolocation)

DROP (hostname geolocation)

[UTwe] OpenIntel (DNS Database)

DDec (hostname geolocation)

Performance measurements

quality of experience assessments

[Ark] border mapping (ISP border mapping)

[Ark] TSLP (time-series latency probing)

[Ama] Mech Turk (crowdsourcing QOE assisment)

[FCC] MBA (latency/performance)

inter-domain links DB (ISP border IPs)

congestion DB (ISP border delay)

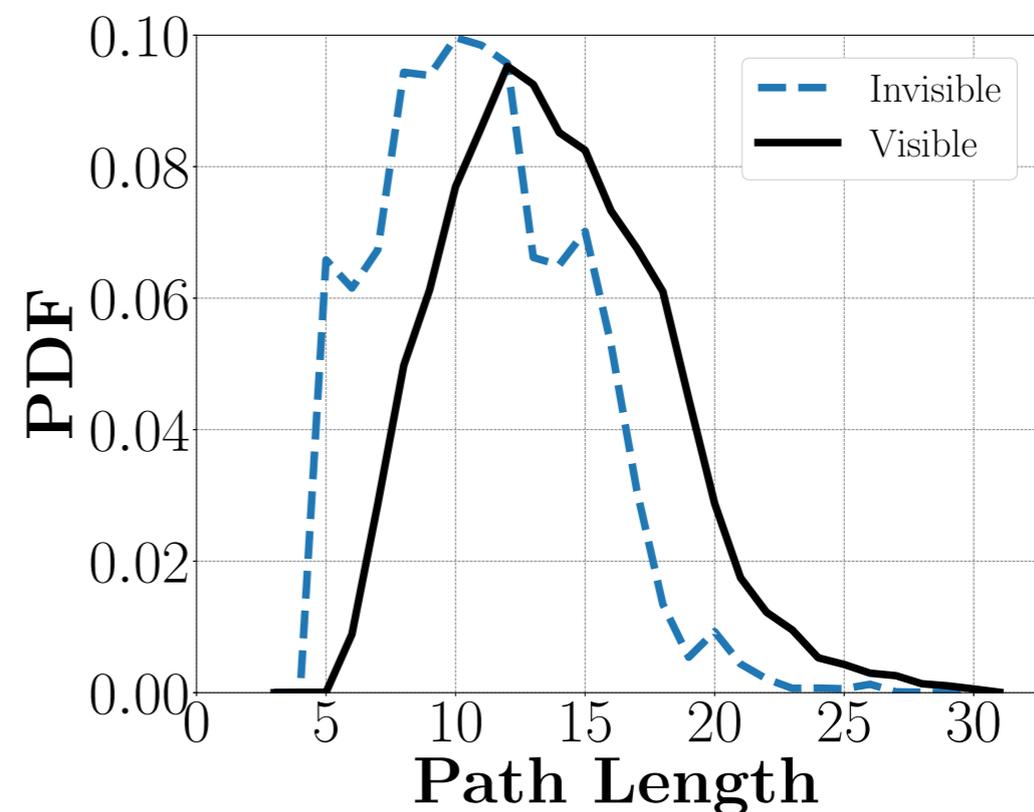
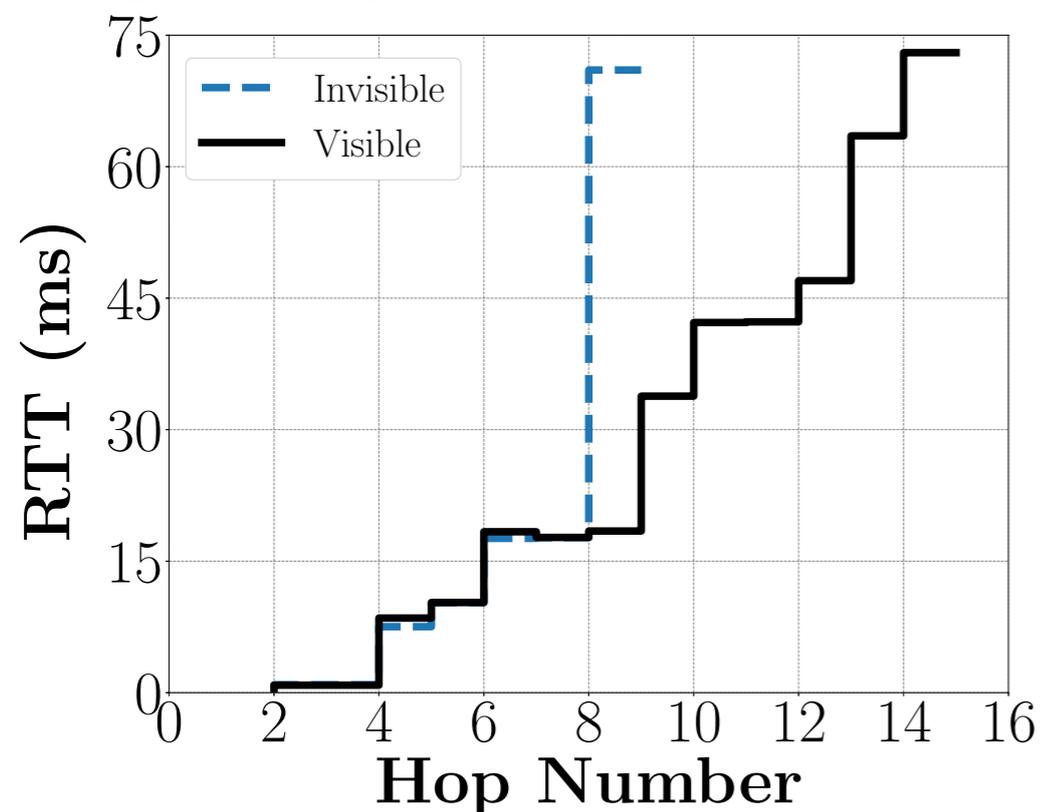
Passive traffic analytics

measuring internet traffic



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)



P
A
N
D
A

G
A
T
E
W
A
Y

Security assessments

testing network vulnerability

[Ark] Spoofer traces
[User,WaiU] netstinky (checks protocol compliance)
[User,UPisa] home traffic (not yet, evaluation phase)

[Spfr] Spoofer DB (detect false address filtering)

tracebox (implemented in Scamper)

Topology measurement IP level

path and performance measurement: IP level

[Ark] servers (traceroutes)
[MIPAR] MIPAR (router aliases)
[RIPE] RIPE Atlas (traceroute,ping)
[Op] Looking Glass Servers (third party traceroute/ping)
[PDB] IX DB (Internet eXchanges)
[CS] IX DB (Internet eXchanges)
[PCH] IX DB (Internet eXchanges)
[HE] IX DB (Internet eXchanges)

[Ark] Ark traceroutes files (IP paths)

[Ark] ITDK files (router topology)

postprocessed data

Topology measurement AS Level

routing measurement data : AS Level

[Ark] ISP-level traceroute (IP paths to AS paths)
[RIPE,RV] BGP data (AS's paths and prefixes)

AS Relationships files (ISP business types)

[AR] AS Rank (AS info and ranking)

Prefix2AS files (AS's prefixes)

AS Link Geo files (inter-AS link with geolocation)

AS Geolocation files (location of ASes)

Customer Cone files (AS's customers)

AS2Org files (Organization's AS)

[BS] BGPStream DB (AS and prefix paths)

Meta-data to support analytics

geographic location of Internet resources

[Max] Maxmind Lite (IP geolocation)

[DE] Netacuity (IP geolocation)

DROP (hostname geolocation)

[UTwe] OpenIntel (DNS Database)

DDec (hostname geolocation)

Performance measurements

quality of experience assessments

[Ark] border mapping (ISP border mapping)

[Ark] TSLP (time-series latency probing)

[Ama] Mech Turk (crowdsourcing QOE assisment)

[FCC] MBA (latency/performance)

inter-domain links DB (ISP border IPs)

congestion DB (ISP border delay)

Passive traffic analytics

measuring internet traffic



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. Graillet, 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)



P
A
N
D
A

G
A
T
E
W
A
Y

Security assessments

testing network vulnerability

[Ark] Spoofer traces
[User,WaiU] netstinky (checks protocol compliance)
[User,UPisa] home traffic (not yet, evaluation phase)

[Spfr] Spoofer DB (detect false address filtering)

tracetun (implemented in Scamper)

Topology measurement IP level

path and performance measurement: IP level

[Ark] servers (traceroutes)
[MIPAR] MIPAR (router aliases)
[RIPE] RIPE Atlas (traceroute,ping)
[Op] Looking Glass Servers (third party traceroute/ping)
[PDB] IX DB (Internet eXchanges)
[CS] IX DB (Internet eXchanges)
[PCH] IX DB (Internet eXchanges)
[HE] IX DB (Internet eXchanges)

[Ark] Ark traceroutes files (IP paths)

[Hen] Henya DB (10 years of traceroute data)

[Ark] ITDK files (router topology)

[Vela] Vela (IP paths)

[Per] Periscope DB (traceroute/ping/BGP)

Improved router topology

IX DB (Internet eXchanges)

Topology measurement AS Level

routing measurement data : AS Level

[Ark] ISP-level traceroute (IP paths to AS paths)
[RIPE,RV] BGP data (AS's paths and prefixes)

AS Relationships files (ISP business types)

Prefix2AS files (AS's prefixes)

AS Link Geo files (inter-AS link with geolocation)

AS Geolocation files (location of ASes)

Customer Cone files (AS's customers)

AS2Org files (Organization's AS)

[AR] AS Rank (AS info and ranking)

[RIR] WHOIS data (Internet ID ownership)

[BS] BGPStream DB (AS and prefix paths)

Meta-data to support analytics

geographic location of Internet resources

[Max] Maxmind Lite (IP geolocation)

[DE] Netacuity (IP geolocation)

DROP (hostname geolocation)

[UTwe] OpenIntel (DNS Database)

DDec (hostname geolocation)

Performance measurements

quality of experience assessments

[Ark] border mapping (ISP border mapping)

[Ark] TSLP (time-series latency probing)

[Ama] Mech Turk (crowdsourcing QOE assisment)

[FCC] MBA (latency/performance)

inter-domain links DB (ISP border IPs)

congestion DB (ISP border delay)

Passive traffic analytics

measuring internet traffic



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