Collaborative Open Source: MANRS Validator

Leslie Daigle
RIPE Open Source WG, October 2019

Overview

- Collaboration and Open Source Software – general remarks

- Pilot project!

- Further discussion

Collaboration & OSS

General Remarks

Collaboration and Open Source Software

Open Source Software

is

Collaboration

Isn't it?

Collaboration and OSS (big projects)

Open Source Software

is

Collaboration

BIRD
Quagga
OpenNFV

…

Engage in established platforms and work out technical details through governance framework

Collaboration and OSS
(little projects)

Open Source Software

is

Collaboration

An individual's bright idea for improving Internet networking….

Hackathon?

< *crickets* >

Collaboration and OSS (theory)

- Sometimes, the software is easier to write than the collaboration is to find
  - Which limits the scope of what can be achieved

Hypothesis: *some of these important projects would be more likely to happen/succeed if they had a framework to support them*

Test: *a pilot project for the MANRS (Mutually Agreed Norms for Routing Security) effort*

Organization

People involved

Coordination required

Idea

Concrete and tractable proposal

Resources to implement

Validate, generalize, expand

MANRS Validator

Pilot Project!

Context

- MANRS – a group of engineers from participating networks
  - Committed to making sure their networks are managed well, and to promote the same for others

- MANRS provides a manifesto
  - Text, commitments
  - Difficult to measure objectively, independently

- What about building a tool to validate router configurations against the manifesto?

Timeline

- "I have an idea for an OSS tool!" – Rich Compton
  - < *crickets* >

- Pilot project/coordination
  - "Here's a vision statement", "And some concrete tests" – Rich Compton
  - Preliminary implementation

The implementation

- Robot Framework, specific tests for each router vendor and MANRS compliance requirement

Sample output

```
-----------------------------------------------------------------------------------------
ACLs being applied to single homed stub customers to prevent them ... | FAIL |
'set interfaces et-0/0/0 description "CWDM4 testing"set interfaces et-0/0/0 unit 0 family inet address 192.168.1.2/24
' does not contain 'inet6 filter input'
-----------------------------------------------------------------------------------------
Are inbound routing advertisements from customers and peers secure... | PASS |
-----------------------------------------------------------------------------------------
Are inbound routing advertisements restricted to only /24 and shor... | PASS |
-----------------------------------------------------------------------------------------
Are inbound routing advertisements restricted to only /48 and shor... | PASS |
-----------------------------------------------------------------------------------------
Are inbound routing advertisements secured by applying AS-path fil... | PASS |
-----------------------------------------------------------------------------------------
Are outbound routing advertisements to peers and transit secured b... | PASS |
-----------------------------------------------------------------------------------------
Is the router configured to connect to a RPKI-to-Router interface ... | PASS |
-----------------------------------------------------------------------------------------
Is the router configured to drop RPKI invalids?                      | PASS |
-----------------------------------------------------------------------------------------
Are communities applied to routes recieved from customers? Are out... | PASS |
-----------------------------------------------------------------------------------------
Is BGP TTL security (GTSM) applied to all BGP sessions?              | FAIL |
```

Screenshot courtesy Rich Compton & Pratik Lotia

Reports

Check Cfg. **Is there control plane policing enabled on TCP port 179 - IPv6?**			yes	**FAIL**	ignore_case=True: 'admin@ENWECORZB0J-BCR04> show configuration | display set set version 17.4R1-S4.2 set groups re0 interfaces em0 unit 0 family inet address 10.240.32.27/23 set groups re0 interfaces em0 unit 0 family inet6 address 2605:1c00:50f3:67::32:27/64 set groups re0 routing-options static route 0.0.0.0/0 next-hop 10.240.32.1 deactivate groups re0 routing-options static route 0.0.0.0/0 set groups re0 routing-options static route 172.30.104.0/24 next-hop 10.240.32.1 set groups re0 routing-options static route 172.30.105.0/24 next-hop 10.240.32.1 set groups re1 interfaces em0 unit 0 family
Check Cfg. **uRPF check on all interfaces - IPv4**			yes	**FAIL**	'set interfaces et-0/0/0 description "CWDM4 testing"set interfaces et-0/0/0 unit 0 family inet address 192.168.1.2/24 ' does not contain 'inet rpf-check'
Check Cfg. **uRPF check on all interfaces - IPv6**			yes	**FAIL**	'set interfaces et-0/0/0 description "CWDM4 testing"set interfaces et-0/0/0 unit 0 family inet address 192.168.1.2/24 ' does not contain 'inet6 rpf-check'
Check Cfg. **Are communities applied to routes recieved from customers? Are outbound filters applied to match only routes carrying the correct commmunity attribute?**			yes	**PASS**	
Check Cfg. **Are inbound routing advertisements from customers and peers secured by applying prefix-level filters?**			yes	**PASS**	
Check Cfg. **Are inbound routing advertisements restricted to only /24 and shorter for IPv4?**			yes	**PASS**	
Check Cfg. **Are inbound routing advertisements restricted to only /48 and shorter?**			yes	**PASS**	

Screenshot courtesy Rich Compton & Pratik Lotia

What we have

- A first implementation

- The MANRS Validator provides objective tooling to review conformance to the manifesto

- Current OSS is set up for:
  - Juniper routers
  - Assuming a single router reflects all the config needed to meet MANRS' requirements

What we're looking for

- Is this useful to operators?

- Extending the existing tool to handle other vendors' routers
  - E.g., Mikrotik

- Extending the logic to accommodate different network configurations
  - E.g., if distribution of routing security implementation across multiple edge routers
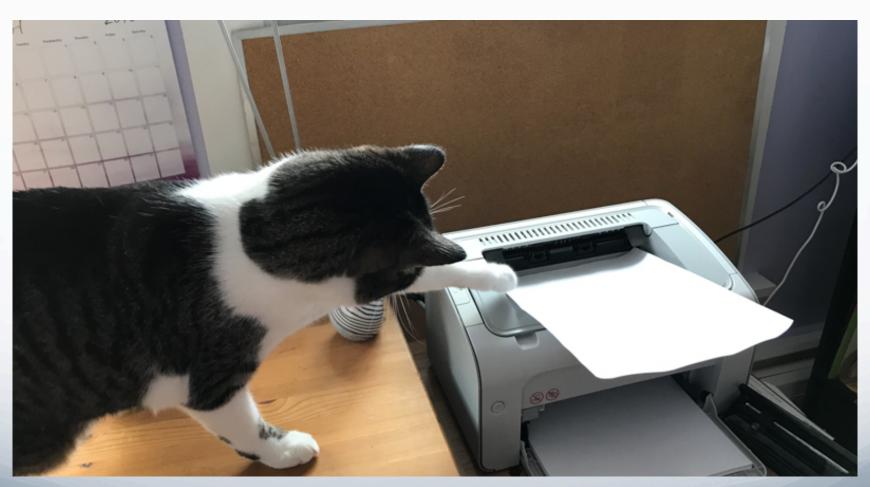
Where you can sign up

- Talk to us this week!
  - Andrei Robachevsky – MANRS project
  - Leslie Daigle -- ldaigle@thinkingcat.com

Further Discussion

What are we saying?

- Clearly there are useful operational tools to be built through collaborative open source

- And, it would be better if that included operator involvement
  - To ensure requirements are understood
  - To ensure it's usable in the end!
  - To prevent the wrong sort of expertise dominating the technical work

Wrong sort of expertise…

The larger context: Operators and Open Source

- That's a *pilot project*
  - Looking to learn more about cross-industry collaboration on projects for operational issues

- Also interested in understanding better what does/ does not work for operators with open source software
  - Using it
  - Helping to build it
  - $upporting it

Thanks!

I have questions! If you have answers, please share:

https://possie.techark.org/ operators-and-open-source- software-survey/