draft-morais-iotops-inxu-01: Intra-Network eXposure analyzer Utility Specification

Sávyo Morais

IOTOPS - IETF 114

LabNet

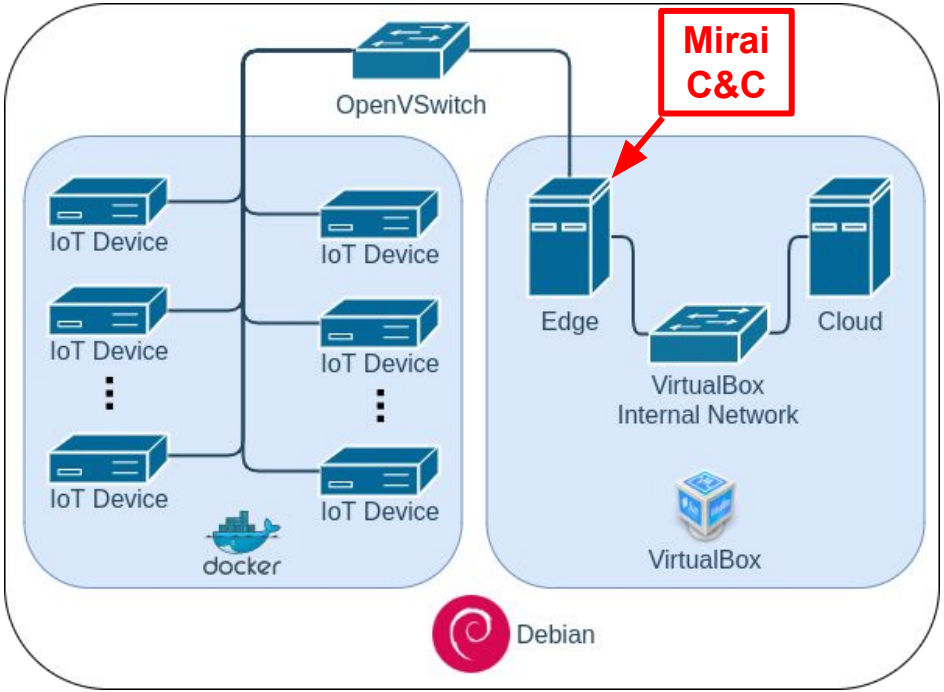
INSTITUTO FEDERAL
Rio Grande do Norte

Agenda

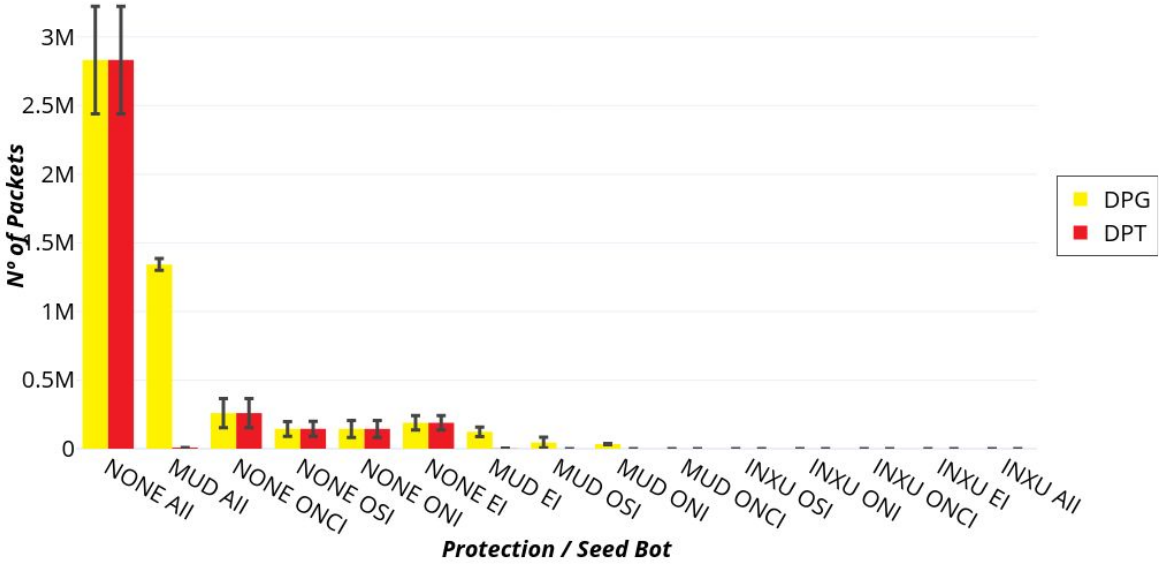
1. *In vitro* experiment - a running code test
2. Experiment results
3. Deployment in other IoT domains - Discussion
4. Next Steps

In vitro experiment - a running code test

- 112 (simulated) IoT devices
  - Docker Busybox images
  - Vulnerable Telnet servers
- MUD files provided by Mudgee
- A Mirai variant



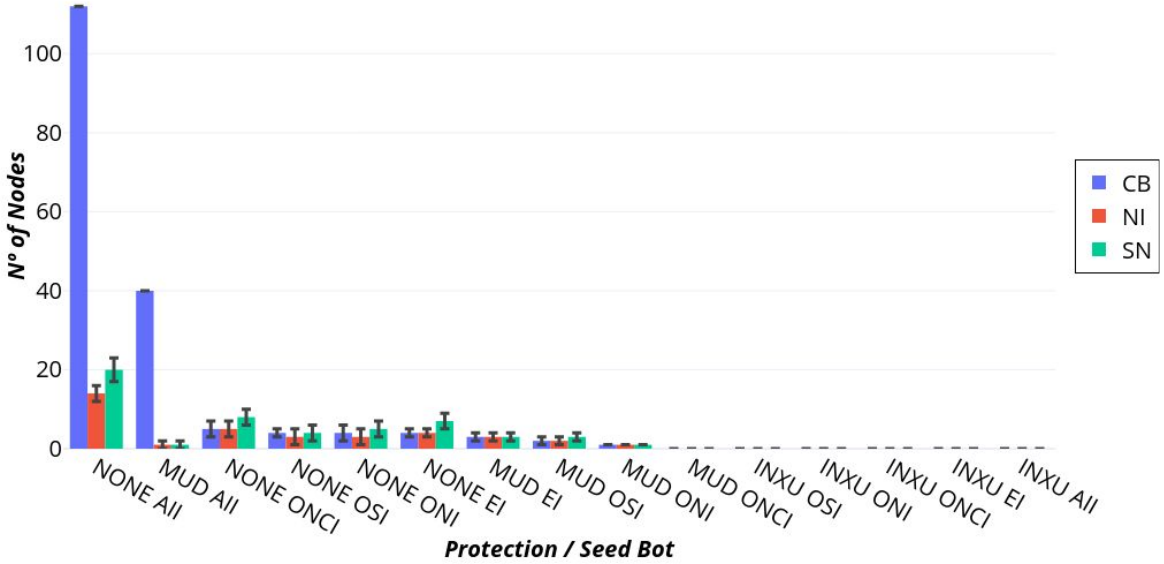
In-vitro tests with a Mirai variant 1/3



Legend:

- Data
  - DPG = DDoS Packets Generated
  - DPT = DDoS Packet Transmitted
- Network Scenario:
  - NONE = Unprotected Network
  - MUD = MUD protection
  - INXU = INXU protection
- Initial Infection Scenario:
  - AII = All IoT hosts Infected
  - EI = Edge node Infected
  - ONCI = One not scannable IoT host infected
  - OSI = One scannable IoT host infected

In-vitro tests with a Mirai variant 2/3



Legend:

- Data
  - CB = Controllable bots
  - NI = New Infections
  - SN = Scanned nodes
- Network Scenario:
  - NONE = Unprotected Network
  - MUD = MUD protection
  - INXU = INXU protection
- Initial Infection Scenario:
  - AII = All IoT hosts Infected
  - EI = Edge node Infected
  - ONCI = One not scannable IoT host infected
  - OSI = One scannable IoT host infected

In-vitro tests with a Mirai variant 3/3

INXU relative gain over MUD

Seed	CB	NI	SN	DPG	DPT
AII	35.75%	7.69%	7.11%	47.40%	0.29%
EI	60.47%	60.47%	44.62%	65.42%	0.91%
ONCI	0.00%	0.00%	0.00%	0.00%	0.00%
ONI	25.00%	25.81%	16.00%	23.29%	0.00%
OSI	64.86%	63.33%	66.67%	30.93%	0.00%

Deployment in other IoT Domains

- Smart Cities
  - Similar topologies and heterogeneity of devices
  - Also has small SOCs taking care of big infrastructures
  - Higher understanding of running applications
  - More computer power available
- Industrial IoT
  - Critical systems
  - Full understanding and control of running applications
  - Deployment over MODBUS/PROFIBUS under study

Next Steps

- INXU as an optimization of anomaly detection:
  - Use INXU output to filter the input data of anomaly detection algorithms
  - Test different approaches for profiling device's traffic
- Improving INXU
  - Reinforce protection of DNS systems
  - Deploy in *real world* for measuring impacts on usability

The End

Questions? Comments?
Suggestions?

INXU I-D:

https://datatracker.ietf.org/doc/draft-morais-iotops-inxu

Papers:

https://sol.sbc.org.br/index.php/wpietf/article/view/13792

https://ieeexplore.ieee.org/abstract/document/9579390/

Contact:

savyovm@gmail.com

savyo.morais@ifrn.edu.br

savyo.morais@labnet.nce.ufrj.br

LabNet

INSTITUTO FEDERAL
Rio Grande do Norte