# Fast responses to new vulnerabilities in Home IoT

Sávyo Morais, T2TRG

draft-morais-iotops-inxu-00

LabNet

Universidade Federal do Rio de Janeiro

# The ongoing issues in Home IoT Insecurity

- Attacks involving these devices are imperceptible to the end-users
- Despite its small impact for individuals, Mirai showed how joining small pieces can be harmful for the Internet
- In a community approach, responding to new vulnerabilities is a slow process
- How can we speed up these responses?

# Is using IDS/IPS a possible answer?

Yes and No. Both signature and anomaly based approaches have some issues for the Home IoT:

- Signature-based:
  - Demands frequent updates of the signatures to ensure protection against new threats
  - Requires technical expertise for fine-tuning rules
    - May expose private data to third parties
- Anomaly Detection:
  - High computational costs for profiling devices
  - An infected device may present malicious behavior during  the profiling process

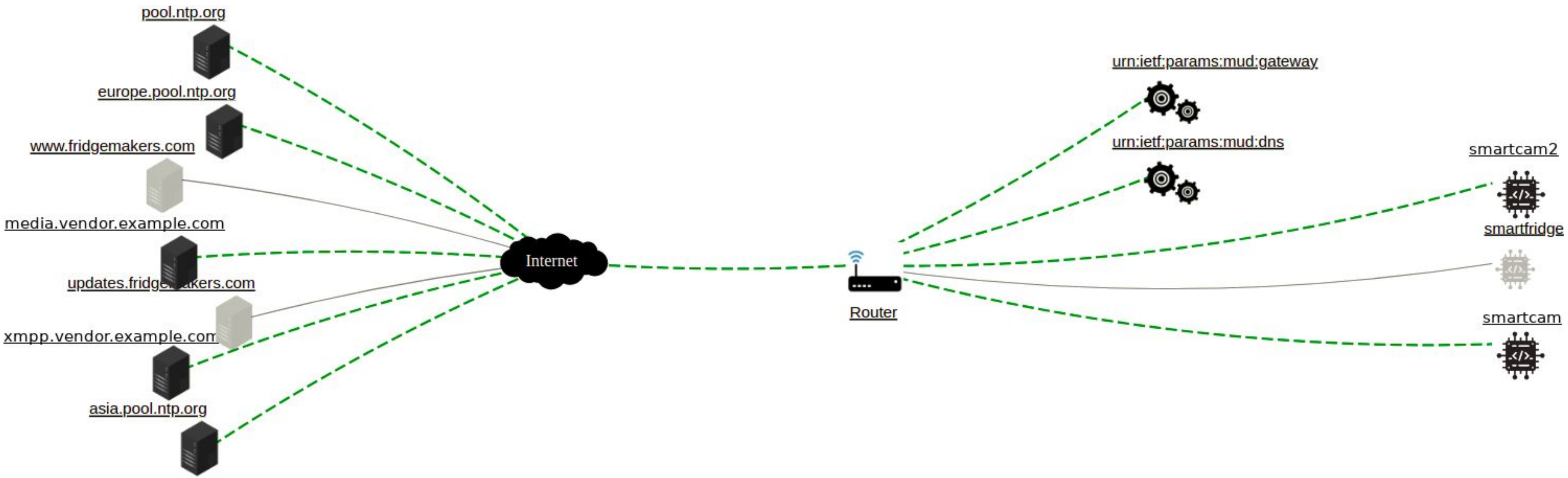
LabNet

Universidade Federal do Rio de Janeiro

# MUD [RFC 5820] as a useful tool

- Pros:
  - Reduces the devices' attack/threat surface
  - Generates a network communication graph that supports threats identification
- Cons:
  - The reliance remains only in the hands of the manufacturer
  - Many devices have a life after the end-of-life

# MUD’s basic functioning




adapted from https://www.mudmaker.org/mudvisualizer.php

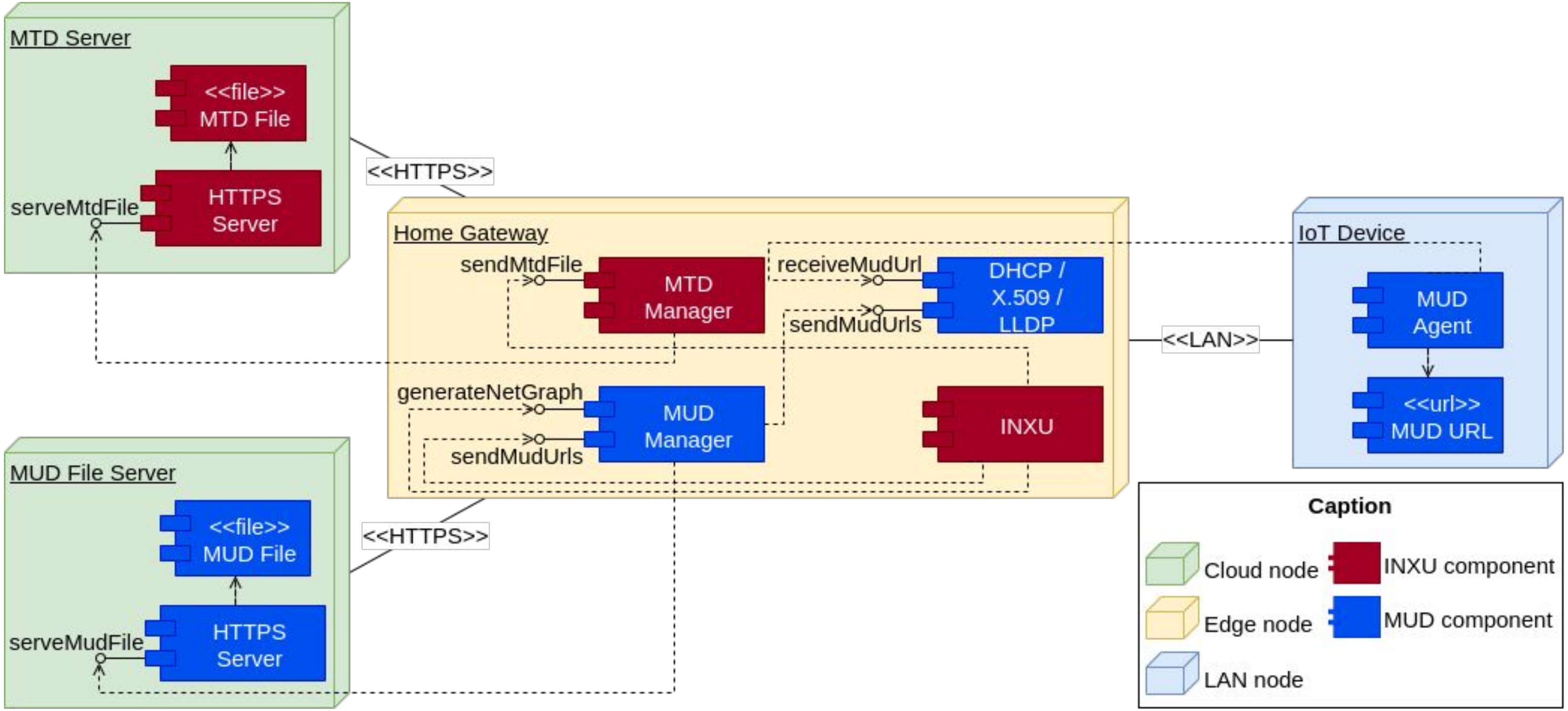
# The draft-morais-iotops-inxu-00

Intra-Network eXposure analyzer Utility is a proposed framework to simplify the process of identification and classification of potential vulnerabilities.

Main features:

- Provides means to give fast responses to new vulnerabilities in Home IoT
- Allows third-party support while keeping end-users’ privacy
- Promotes knowledge sharing for a collective protection

# INXU's Architecture



# The Malicious Traffic Description

- An YANG data model
- Inspired on MUD data model
  - Uses Access Control Lists for describing attack and malware signatures
- Carries context information for proper assessment of the exposure of vulnerabilities
- Simplifies the interpretation of the signatures in distinct networks

# The MTD Data Model

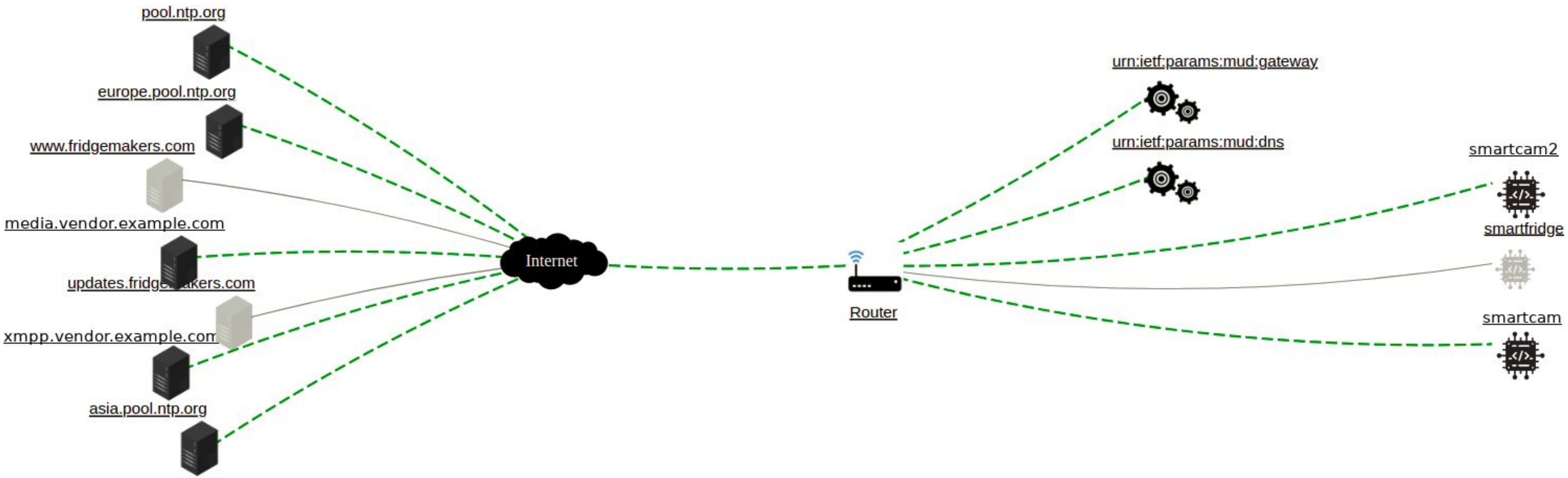
```
+--rw attack-descriptions
|  +--rw to-device-attacks
|  |  +--rw attack-lists
|  |     +--rw attack-list* [name]
|  |        +--rw name                 -> /acl:acls/acl/name
|  |        +--rw specific-devices*    inet:uri
|  +--rw from-device-attacks
|     +--rw attack-lists
|        +--rw attack-list* [name]
|           +--rw name                 -> /acl:acls/acl/name
|           +--rw specific-devices*    inet:uri
```

Attack Description

```
+--rw malware-descriptions
   +--rw malwares-list* [name]
      +--rw name                    string
      +--rw specific-devices*       inet:uri
      +--rw critical-acl-sets* [name]
      |  +--rw name                 string
      |  +--rw critical-acl-set*    -> /acl:acls/acl/name
      |  +--rw action-to-take       ufrj-mtd-2:action-to-take
      +--rw to-device-attacks
      |  +--rw attack-lists
      |     +--rw attack-list* [name]
      |        +--rw name                 -> /acl:acls/acl/name
      |        +--rw specific-devices*    inet:uri
      +--rw from-device-attacks
      |  +--rw attack-lists
      |     +--rw attack-list* [name]
      |        +--rw name                 -> /acl:acls/acl/name
      |        +--rw specific-devices*    inet:uri
      +--rw not-attack-traffic
         +--rw to-device-not-attack-traffic* [name]
         |  +--rw name    -> /acl:acls/acl/name
         +--rw from-device-not-attack-traffic* [name]
            +--rw name    -> /acl:acls/acl/name
```

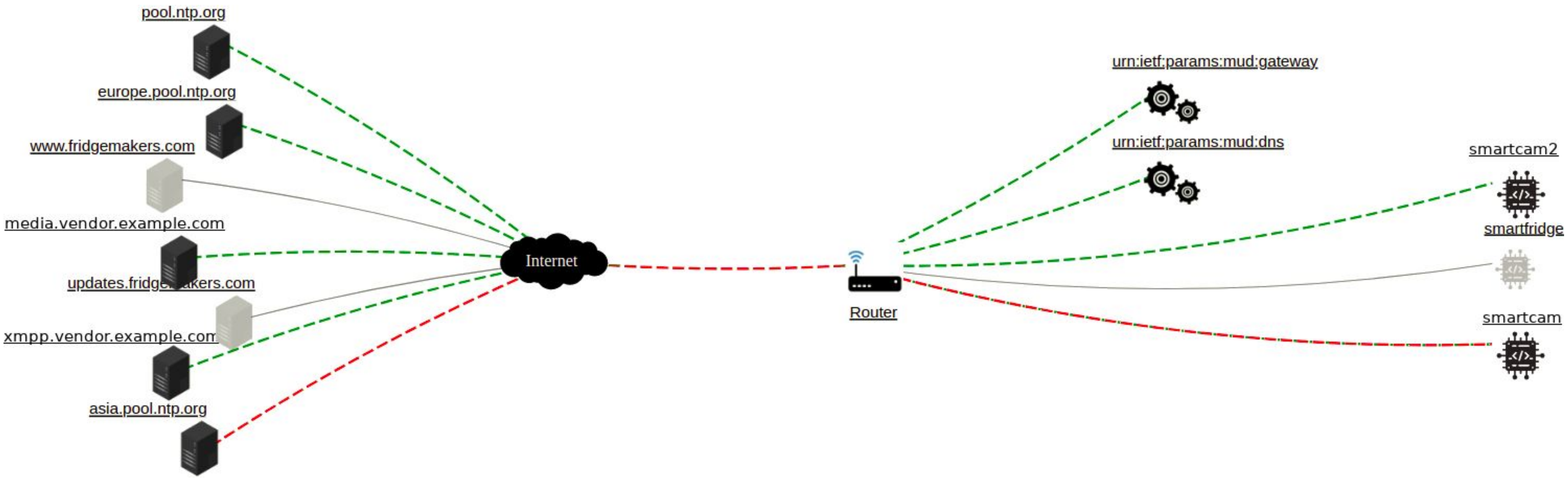
Malware Description

# Identifying and Assessing Vulnerability Exposures - 1/2



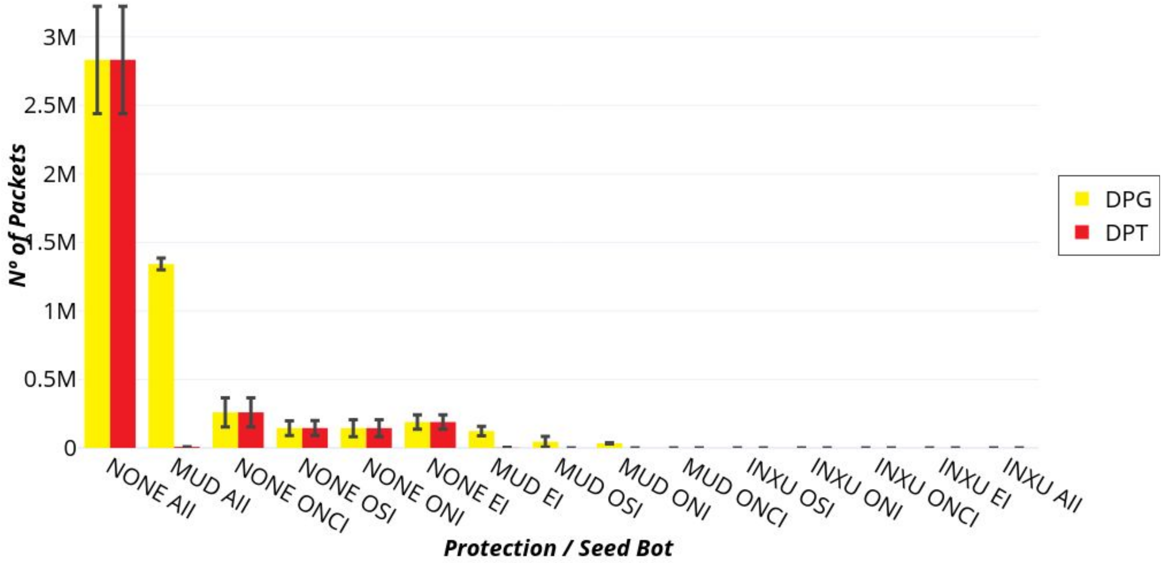

adapted from https://www.mudmaker.org/mudvisualizer.php

# Identifying and Assessing Vulnerability Exposures - 2/2




adapted from https://www.mudmaker.org/mudvisualizer.php

# *In-vitro* tests with a Mirai variant 1/3



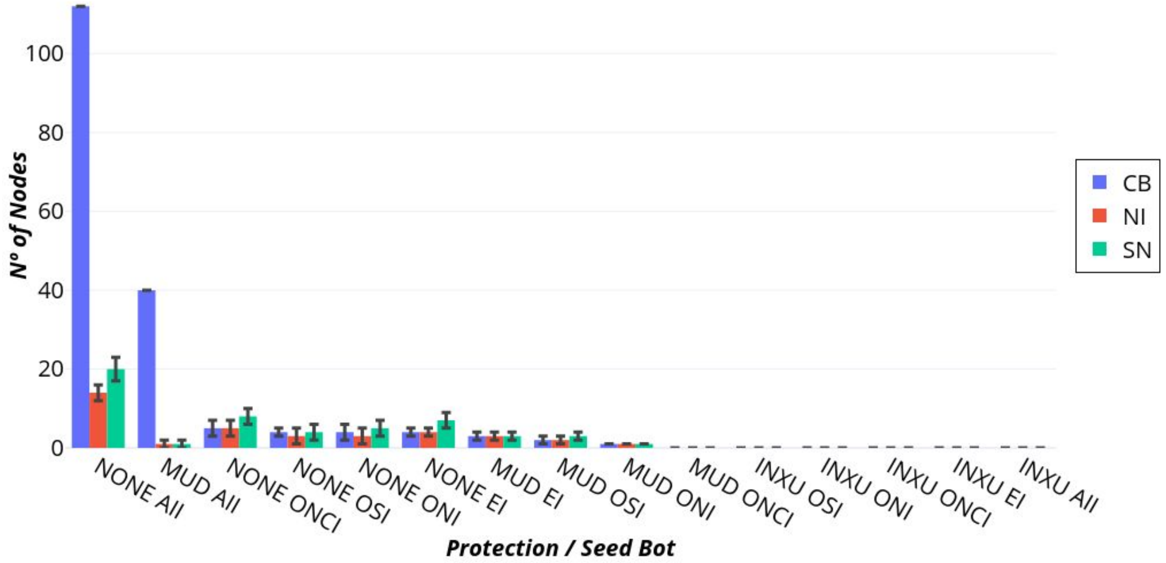

Legend:

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

LabNet

Universidade Federal do Rio de Janeiro

# *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:
  - All = All IoT hosts Infected
  - EI = Edge node Infected
  - ONCI = One not scannable IoT host infected
  - OSI = One scannable IoT host infected

LabNet

Universidade Federal do Rio de Janeiro

# *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% |

LabNet

Universidade Federal do Rio de Janeiro

# Next Steps

- INXU as an optimization of anomaly detection:
  - Use INXU output as an input filter 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
- Ongoing undergraduate thesis on collective malware profiling
  - Keeping end-user privacy
  - Automatic generation of MTD files

# The Starting

Of a long journey of questions, comments, and improvements

INXU I-D:

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

Contact:

savyovm@gmail.com

LabNet

Universidade Federal do Rio de Janeiro