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

Sávyo Morais

OPSAWG - IETF 114

LabNet

INSTITUTO FEDERAL
Rio Grande do Norte

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?

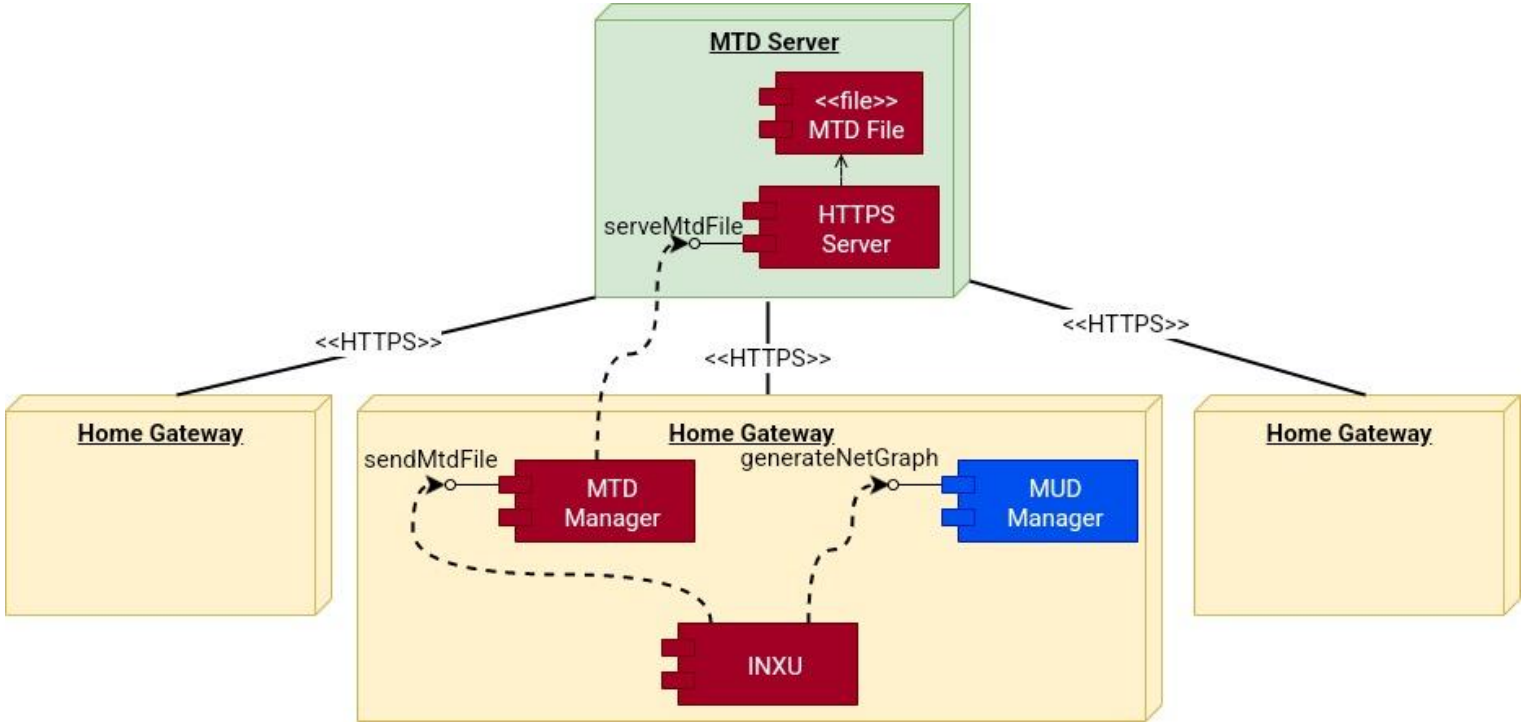
The draft-morais-iotops-inxu-01

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



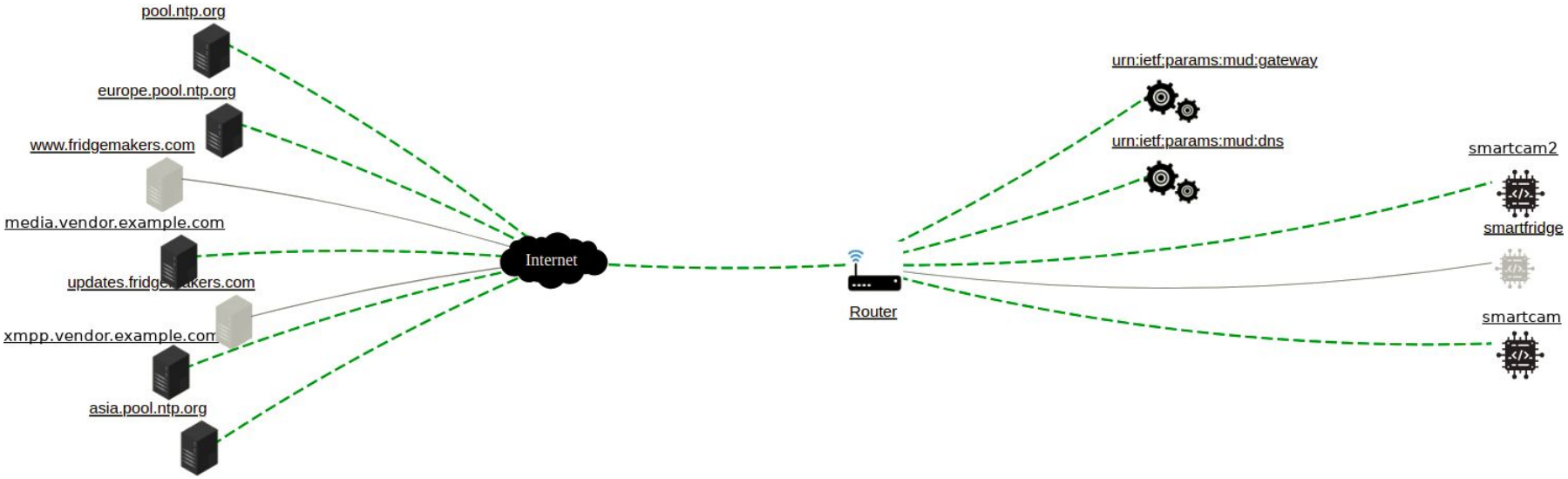
The Malicious Traffic Description

- 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

The MTD Data Model

```
+--rw malicious-descriptions
   +--rw malicious-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          draft-inxu-mtd:action-to-take
      +--rw to-device-attacks
      |  +--rw traffic-lists
      |     +--rw traffic-list* [name]
      |        +--rw name                   -> /acl:acls/acl/name
      |        +--rw specific-devices*      inet:uri
      +--rw from-device-attacks
      |  +--rw traffic-lists
      |     +--rw traffic-list* [name]
      |        +--rw name                   -> /acl:acls/acl/name
      |        +--rw specific-devices*      inet:uri
      +--rw to-device-not-attacks
      |  +--rw traffic-lists
      |     +--rw traffic-list* [name]
      |        +--rw name                   -> /acl:acls/acl/name
      |        +--rw specific-devices*      inet:uri
      +--rw from-device-not-attacks
         +--rw traffic-lists
            +--rw traffic-list* [name]
               +--rw name                   -> /acl:acls/acl/name
               +--rw specific-devices*      inet:uri
```

Identifying and Assessing Vulnerability Exposures - 1/3



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

Identifying and Assessing Vulnerability Exposures - 2/3

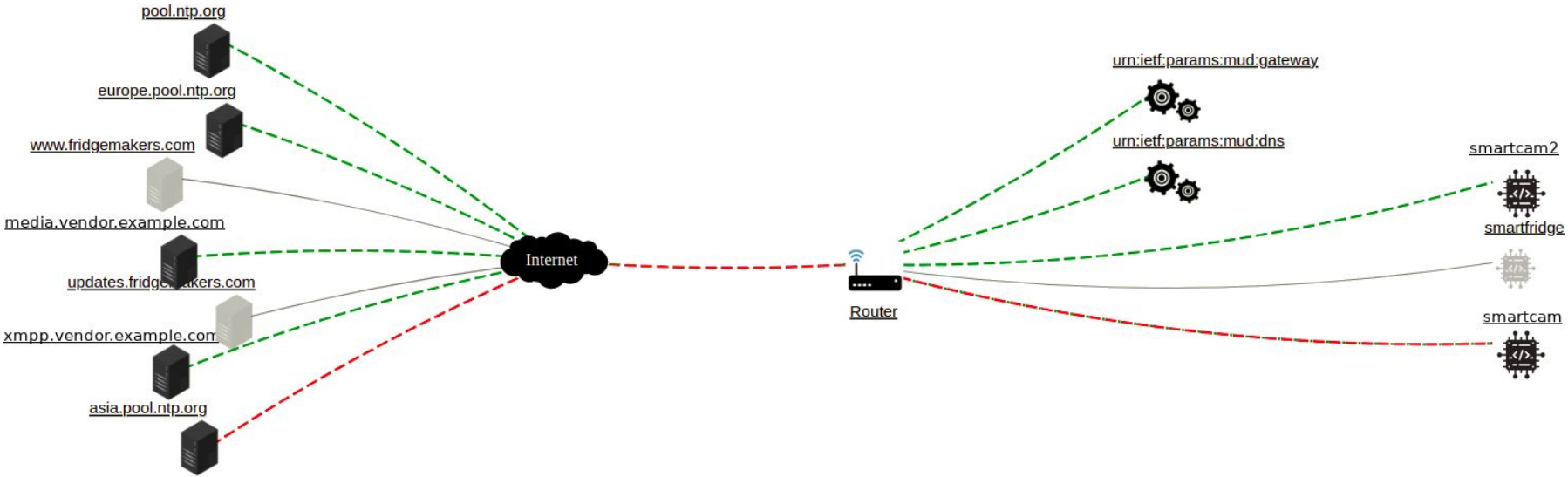
Identifying a vulnerability exposure:

- Source and destination IPs;
- Protocol (ICMP, UDP, or TCP);
- TCP Initiator;
- Transport header:
  - Source and destination ports;
- ICMP header:
  - Type and code

Threat Assessment:

- Sum the risks of the exposed ACEs;
- Classifying the risk of an ACL:
  - Risk Threshold;
  - Alert Threshold;
- Assessing Threats:
  - Critical ACL Set
  - Action to take

Identifying and Assessing Vulnerability Exposures - 3/3



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

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

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