Research and Innovation

# STAR @ CIn-UFPE

Marcelo d’Amorim – damorim@cin.ufpe.br

December 2019

# STAR

## Software Testing and Analysis Research

Breno

Leopoldo

Marcelo

# Goal

Prevent, discover, diagnose, and repair **software bugs** and **vulnerabilities** to improve **software quality**

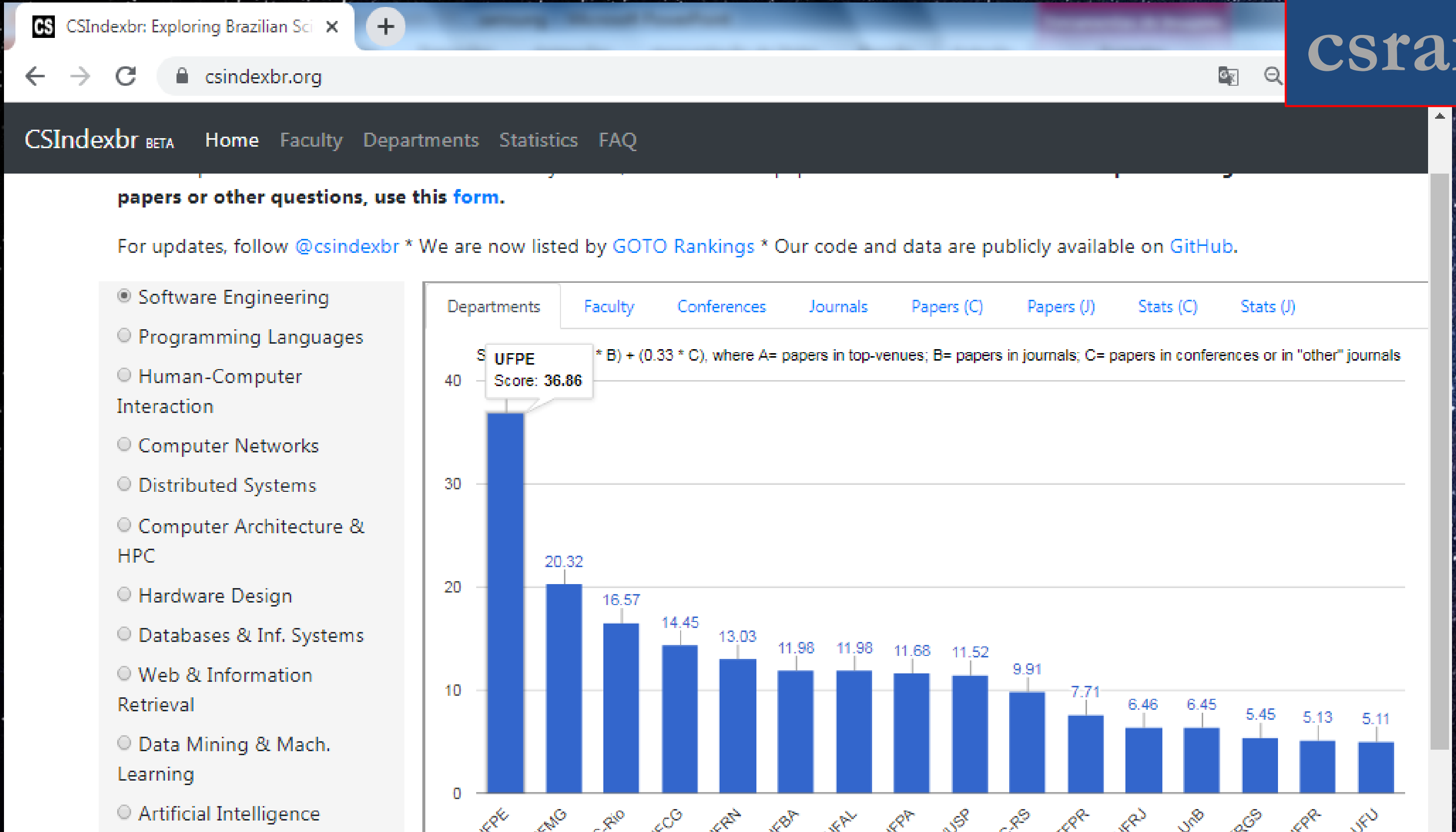
# Achievements

- Found, reported, and fixed hundreds of bugs!
- Developed several popular open-source tools
- Attracted funding from diverse sources (e.g., Microsoft, Facebook, NSF, etc.)
- Published research in highly-selective venues

# Leaders in SE research in Brazil and South America

**csindexbr.org**

**csrankings.org**



CSIndexbr: Exploring Brazilian Sci

csindexbr.org

CSIndexbr BETA Home Faculty Departments Statistics FAQ

papers or other questions, use this form.

For updates, follow @csindexbr * We are now listed by GOTO Rankings * Our code and data are publicly available on GitHub.

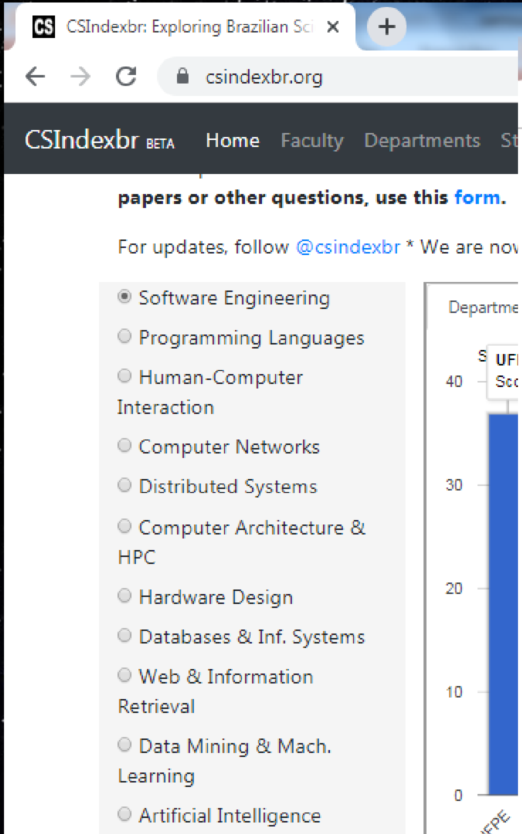
- ● Software Engineering
- ○ Programming Languages
- ○ Human-Computer Interaction
- ○ Computer Networks
- ○ Distributed Systems
- ○ Computer Architecture & HPC
- ○ Hardware Design
- ○ Databases & Inf. Systems
- ○ Web & Information Retrieval
- ○ Data Mining & Mach. Learning
- ○ Artificial Intelligence

S * B) + (0.33 * C), where A= papers in top-venues; B= papers in journals; C= papers in conferences or in "other" journals

# Leaders in SE research in Brazil and South America

csindexbr.org

csrankings.org



CSIndexbr: Exploring Brazilian Sci

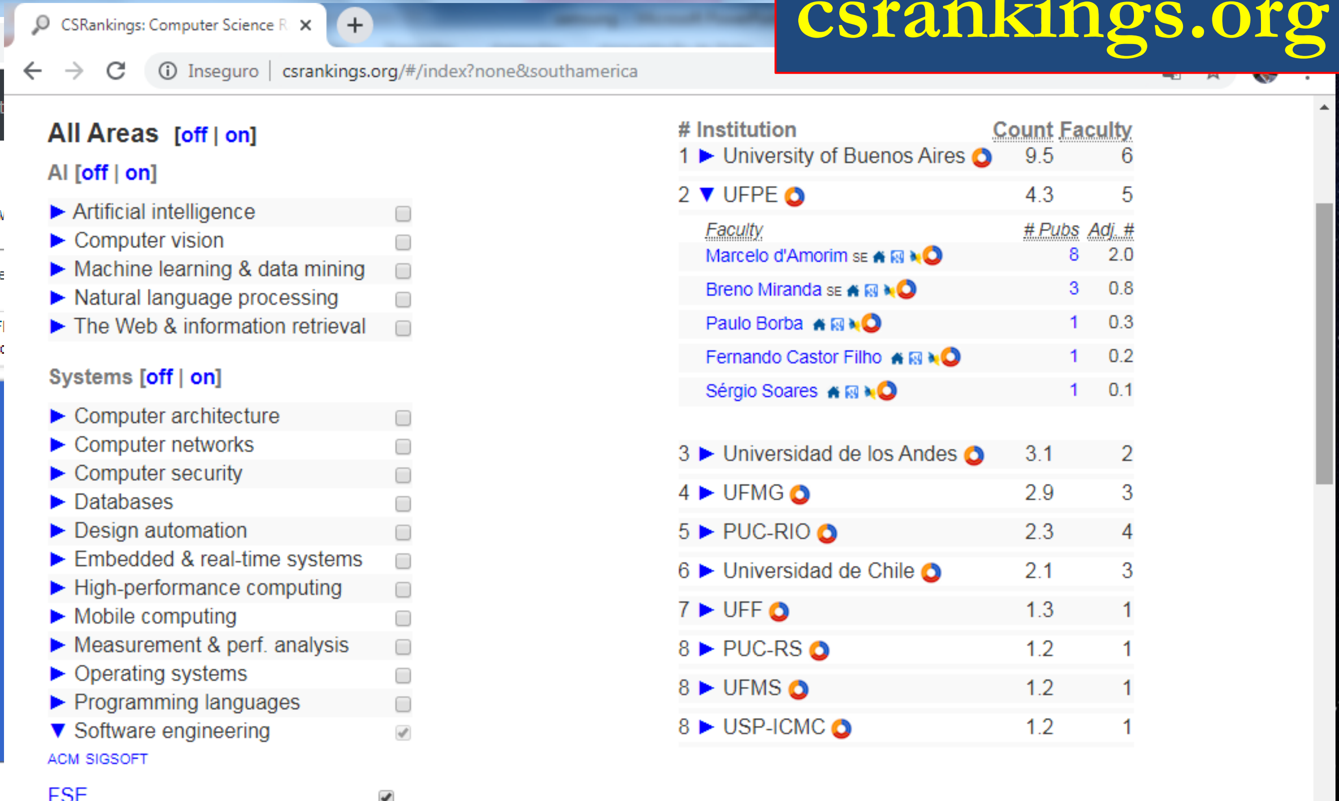
csindexbr.org

CSIndexbr BETA · Home · Faculty · Departments · St

papers or other questions, use this form.

For updates, follow @csindexbr * We are nov

- ● Software Engineering
- ○ Programming Languages
- ○ Human-Computer Interaction
- ○ Computer Networks
- ○ Distributed Systems
- ○ Computer Architecture & HPC
- ○ Hardware Design
- ○ Databases & Inf. Systems
- ○ Web & Information Retrieval
- ○ Data Mining & Mach. Learning
- ○ Artificial Intelligence



CSRankings: Computer Science R

Inseguro | csrankings.org/#/index?none&southamerica

**All Areas** [off | on]

AI [off | on]

- ▶ Artificial intelligence □
- ▶ Computer vision □
- ▶ Machine learning & data mining □
- ▶ Natural language processing □
- ▶ The Web & information retrieval □

Systems [off | on]

- ▶ Computer architecture □
- ▶ Computer networks □
- ▶ Computer security □
- ▶ Databases □
- ▶ Design automation □
- ▶ Embedded & real-time systems □
- ▶ High-performance computing □
- ▶ Mobile computing □
- ▶ Measurement & perf. analysis □
- ▶ Operating systems □
- ▶ Programming languages □
- ▼ Software engineering ☑

ACM SIGSOFT

FSE ☑

| # | Institution | Count | Faculty |
|---|---|---|---|
| 1 | ▶ University of Buenos Aires | 9.5 | 6 |
| 2 | ▼ UFPE | 4.3 | 5 |

| Faculty | # Pubs | Adj. # |
|---|---|---|
| Marcelo d'Amorim SE | 8 | 2.0 |
| Breno Miranda SE | 3 | 0.8 |
| Paulo Borba | 1 | 0.3 |
| Fernando Castor Filho | 1 | 0.2 |
| Sérgio Soares | 1 | 0.1 |

| # | Institution | Count | Faculty |
|---|---|---|---|
| 3 | ▶ Universidad de los Andes | 3.1 | 2 |
| 4 | ▶ UFMG | 2.9 | 3 |
| 5 | ▶ PUC-RIO | 2.3 | 4 |
| 6 | ▶ Universidad de Chile | 2.1 | 3 |
| 7 | ▶ UFF | 1.3 | 1 |
| 8 | ▶ PUC-RS | 1.2 | 1 |
| 8 | ▶ UFMS | 1.2 | 1 |
| 8 | ▶ USP-ICMC | 1.2 | 1 |

Part of a joint US/Brazil Cyber-Security project. Funded by NSF/RNP ($300K).

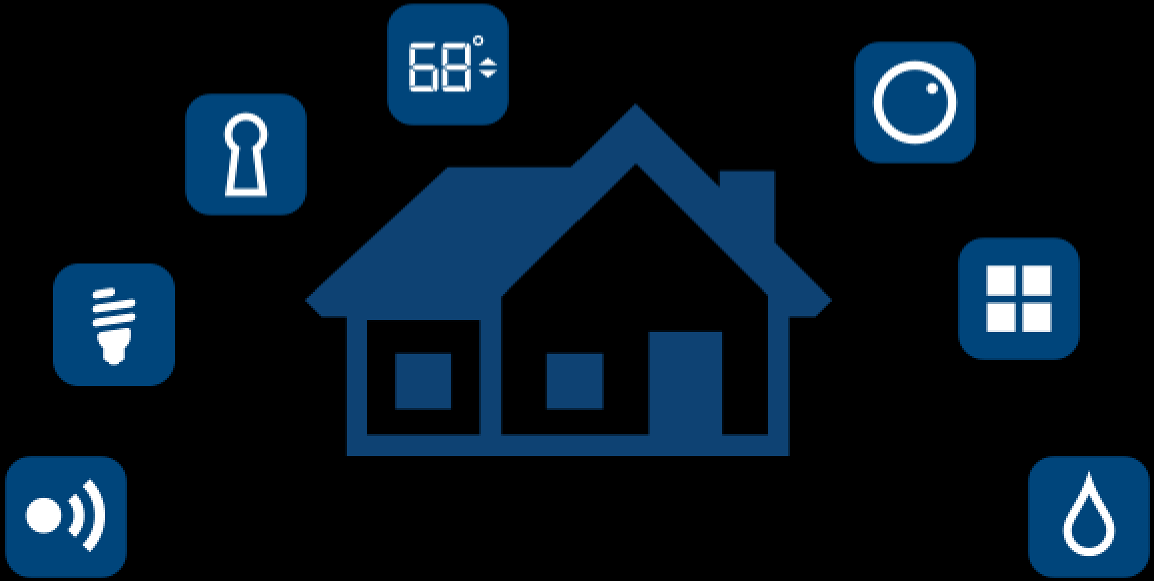
# CASE:
# SECURITY TESTING

Security Testing

- **IoT Security**
- Network Intrusion Detection
- Generation of Drivers to Fuzz

# Internet of Things (IoT) Security

## Context:



Smart Home

# Internet of Things (IoT)

Lots of very simple (and cheap) devices in the market

Bulb

Presence

Smoke

# Internet of Things (IoT)

Often devices are resource-constrained

…as they are relatively cheap (built for the masses)

Bulb

Presence

Smoke

# Internet of Things (IoT)

Often devices are resource-constrained

…as they are relatively cheap (built for the masses)

Challenging to implement robust security mechanisms.

Bulb

Presence

Smoke

# What we did

- Analyzed code of apps of various IoT devices looking for possible security issues
- Used both static and dynamic analysis tools

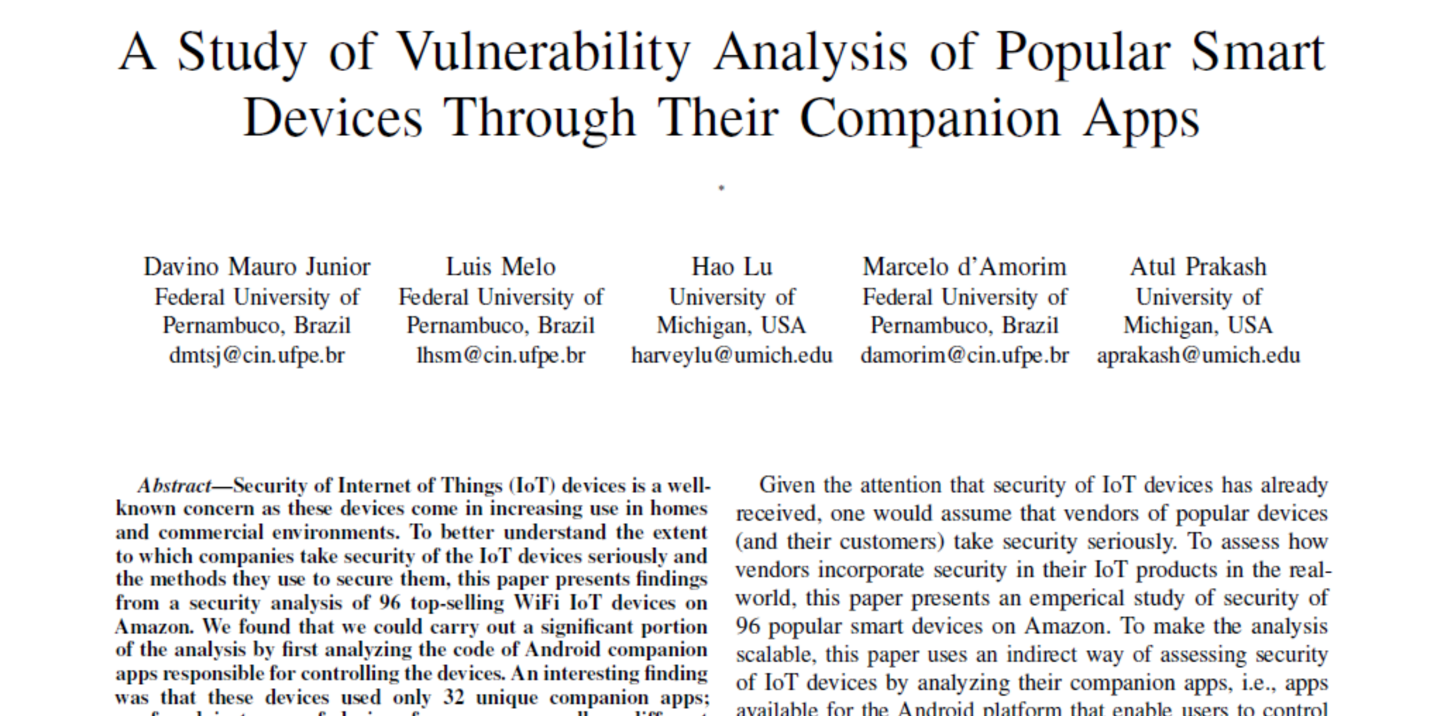
# What we found

Around 50% of apps we analyzed were problematic

- Passwords expressed in code
- Weak crypto algorithms
- etc.

# In the press…

SafeThings2019 (part of Oakland Security)



## A Study of Vulnerability Analysis of Popular Smart Devices Through Their Companion Apps

Davino Mauro Junior
Federal University of Pernambuco, Brazil
dmtsj@cin.ufpe.br

Luis Melo
Federal University of Pernambuco, Brazil
lhsm@cin.ufpe.br

Hao Lu
University of Michigan, USA
harveylu@umich.edu

Marcelo d'Amorim
Federal University of Pernambuco, Brazil
damorim@cin.ufpe.br

Atul Prakash
University of Michigan, USA
aprakash@umich.edu

***Abstract*—Security of Internet of Things (IoT) devices is a well-known concern as these devices come in increasing use in homes and commercial environments. To better understand the extent to which companies take security of the IoT devices seriously and the methods they use to secure them, this paper presents findings from a security analysis of 96 top-selling WiFi IoT devices on Amazon. We found that we could carry out a significant portion of the analysis by first analyzing the code of Android companion apps responsible for controlling the devices. An interesting finding was that these devices used only 32 unique companion apps;**

Given the attention that security of IoT devices has already received, one would assume that vendors of popular devices (and their customers) take security seriously. To assess how vendors incorporate security in their IoT products in the real-world, this paper presents an emperical study of security of 96 popular smart devices on Amazon. To make the analysis scalable, this paper uses an indirect way of assessing security of IoT devices by analyzing their companion apps, i.e., apps available for the Android platform that enable users to control

# In the press…

http://www.cisoadvisor.com.br/iot-expoe-residencias-a-invasores/
https://www.theregister.co.uk/2019/02/04/iot_apps_encryption/
https://nakedsecurity.sophos.com/2019/02/05/half-of-iot-devices-let-down-by-vulnerable-apps/
https://www.techradar.com/news/insecure-apps-put-half-of-iot-devices-at-risk

TechRadar is supported by its audience. When you purchase through links on our site, we may earn an affiliate commission. Learn more

Home > News > Internet

Insecure apps put half of IoT devices at risk

Free to Access, Read and Share
Build Your First Website eBook
In association with GoDaddy

Security Testing

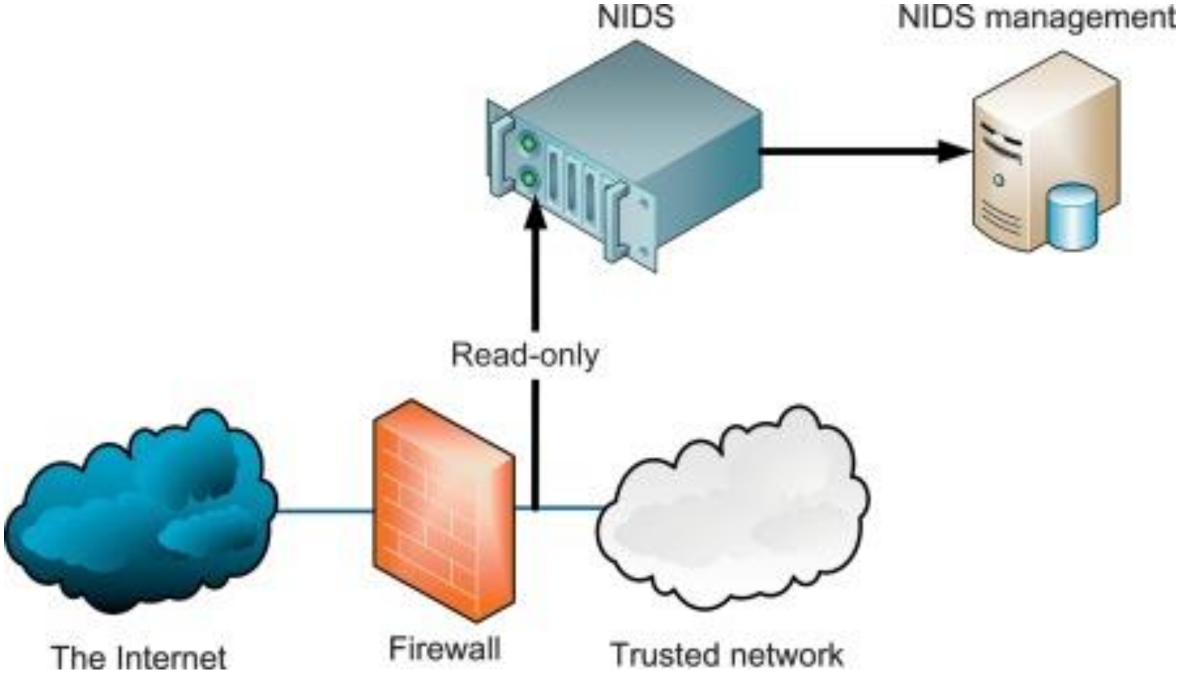
IoT Security

Network Intrusion Detection (ongoing)

Generation of Drivers to Fuzz

# Network Intrusion Detection Systems (NIDS)

Port scan
Spoofing(ARP,IP,DNS)
TCP SYN flood
Data modification
…



# Two main approaches

- Signature-based
- Anomaly-based

# Two main approaches

- **Signature-based**
- Anomaly-based

Most popular open-source NIDS

# How it works…

- Security expert specifies attack pattern
- NIDS checks traffic
- The system or sys admin takes action

# Basic Rule

## Preventing SQL Injection Attack

```
alert tcp any any -> any 80 (msg: "Error Based SQL Injection
Detected"; content: "%27" ; sid:100000011; )
```

Single quote

https://www.hackingarticles.in/detect-sql-injection-attack-using-snort-ids/

# Rule Format

```
alert tcp any any -> any 80 (msg: "Error Based SQL Injection
Detected"; content: "%27" ; sid:100000011; )
```

Action: pass, drop, reject, alert

Header: protocol source-address port [ -> or <-> ] target-address port

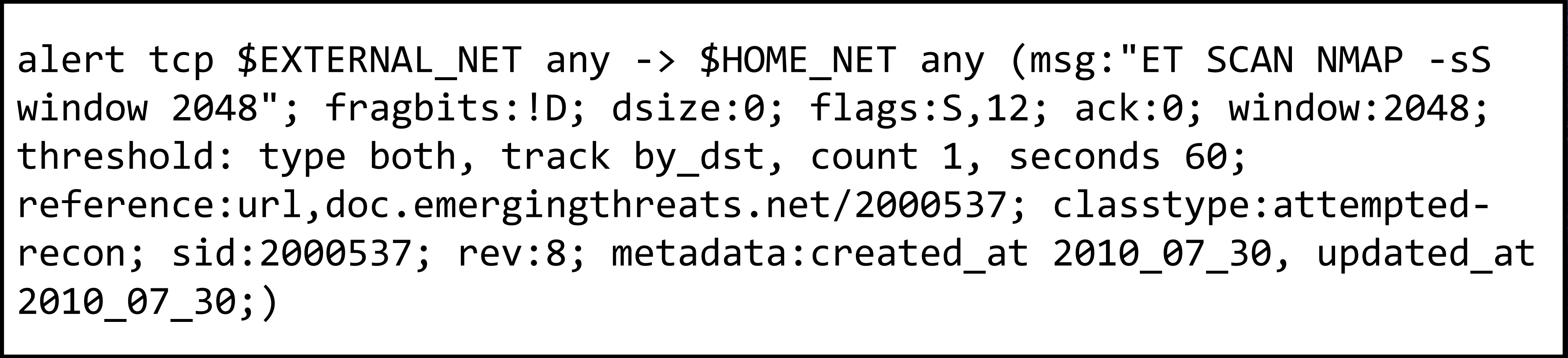
Rule Options: …

https://suricata.readthedocs.io/en/suricata-4.1.4/rules/intro.html

# Observations

- Rules are based on heuristics
- Hundreds of such rules exist (for Suricata: ~200 official, thousands non-official)
- They can get very confusing!

# Observations



```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN NMAP -sS
window 2048"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:2048;
threshold: type both, track by_dst, count 1, seconds 60;
reference:url,doc.emergingthreats.net/2000537; classtype:attempted-
recon; sid:2000537; rev:8; metadata:created_at 2010_07_30, updated_at
2010_07_30;)
```

- They can get very confusing!

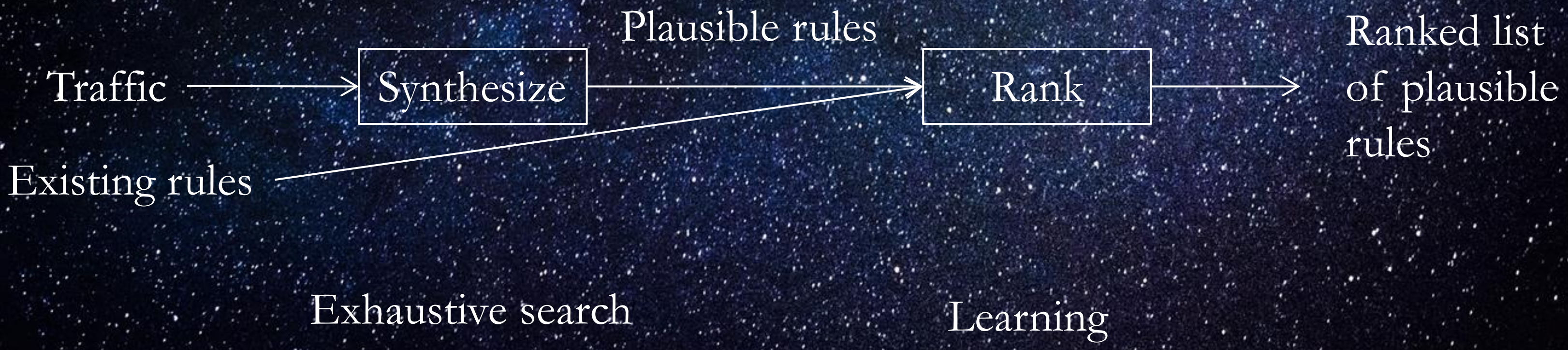
Source: https://security.stackexchange.com/questions/188021/suricata-nmap-scan-does-not-match-rules

# Problem

It is challenging for maintainer to keep up with the pace of attackers

# Our Approach

Synthesize rules from traffic (both benign and malicious) and observations from existing rules



Traffic

Existing rules

Synthesize

Plausible rules

Rank

Ranked list of plausible rules

Exhaustive search

Learning

Security Testing

IoT Security

Network Intrusion Detection

Generation of Drivers to Fuzz (ongoing)

# Other Areas of Interest

- Testing Configurable Systems
- Regression Testing
- Automated Debugging

Research and Innovation

# STAR @ CIn-UFPE

Marcelo d’Amorim – damorim@cin.ufpe.br

More info at **cin.ufpe.br/~damorim**

December 2019