Institut Mines-Télécom

# SMART HOME SECURITY
# NETWORK ANOMALY DETECTION

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

IMT Mines Albi-Carmaux
École Mines-Télécom

IMT Mines Alès
École Mines-Télécom

Institut Mines-Télécom
Business School

MINES Saint-Étienne
Une école de l'IMT

TELECOM Paris
IP PARIS

TELECOM SudParis
IP PARIS

EURECOM

InSIC

## Contributors

This is their work

- Mustafizur R. Shahid (Ph.D, 2017 – 2021)
- Houda Jmila (Postdoc, 2018 – )
- Marwan Lazrag (Engineer, 2019 – )
- Paul-Henri Mignot (Engineer, 2021 – )
- Zujany Salazar (Intern, 2019)

- Supervisors: Gregory Blanc, Hervé Debar, Christophe Kiennert, Zonghua Zhang

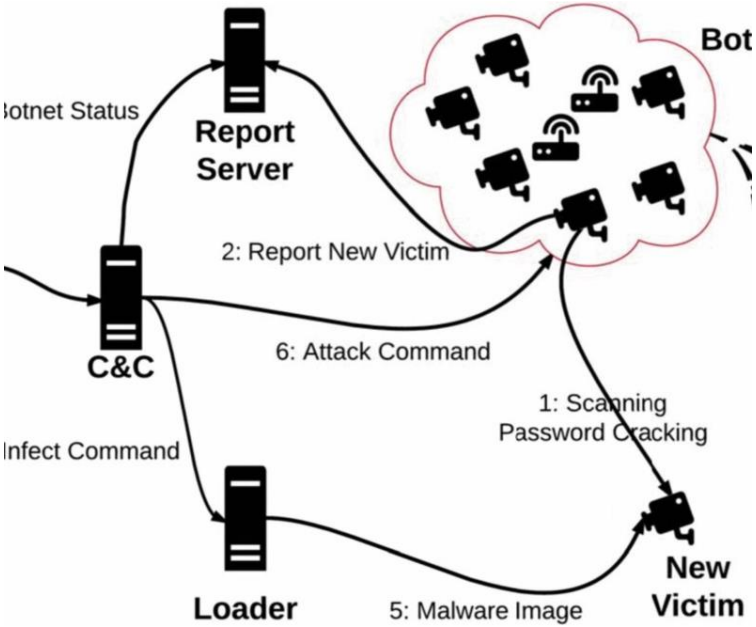
## Projects

They supported this work

- CEF *VARIoT* (Vulnerability and Attack Repository for IoT, 2019 – 2022) funded by HaDEA, a European Commission Agency

- *Futur & Ruptures* (2017 – 2021) is an IMT Ph.D grant
- LTCI/SAMOVAR joint project grant
- H2020 *SPARTA* (2019 – 2022)

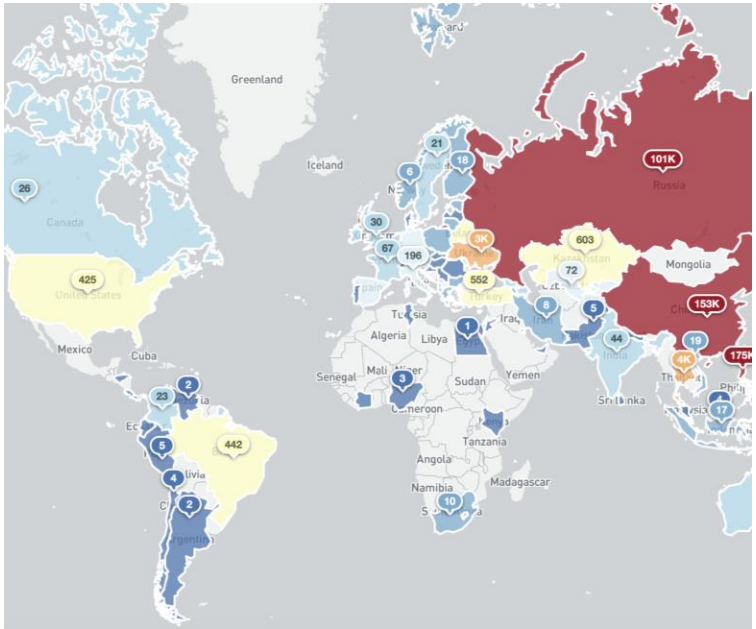
- R3S team, SAMOVAR, Télécom SudParis




## Botnets exploit IoT vulnerabilities

In fall 2016, Mirai successively target Krebs on Security (**620 Gbits/s**), OVH (**1 Tbit/s**) and Dyn (**~100,000 devices**)

- IoT malware thrive on **poorly secured** devices: weak credentials, backdoors, lack of updates
- IoT devices are proliferating: **41.6B** by 2025
- Securing them all is an *illusion* (esp. proprietary software stacks)




## IoT devices expose CoAP service

Since June 2020, Shadowserver publishes **daily CoAP scan reports**

- Scan consists in sending a CoAP GET request for `/.well-known/core` to port UDP/5683 on all routable IPv4 addresses
- CoAP is prone to DDoS amplification (RDDoS) with a factor **34**. CoAP implementations also suffer from known software vulnerabilities leading to **RCE**.
- **464k** devices responded. Top respondents (in red) account for nearly **93%** of the *exposed* instance.

## Datasheet

CEF Telecom – Public Open Data (CEF-TC-2018-5 call)

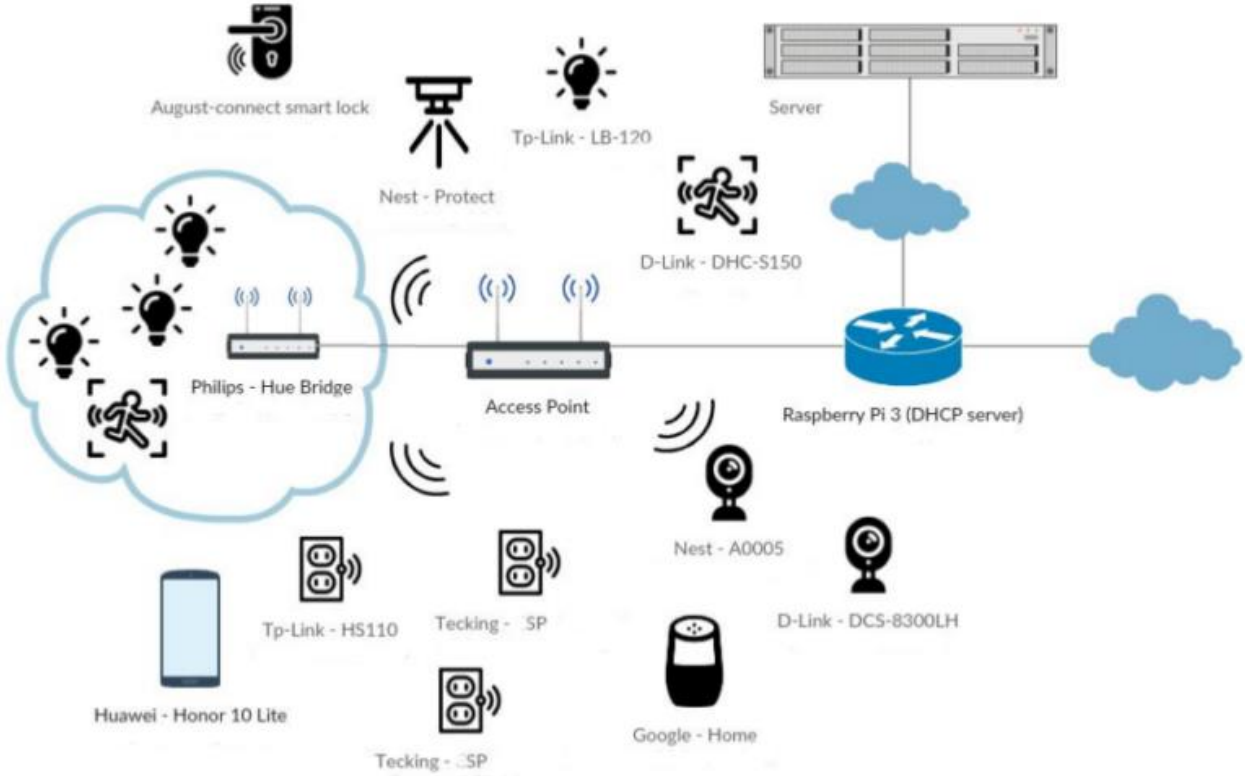
- Start: 07.2019
- End: 10.2022
- Funding agency: HaDEA

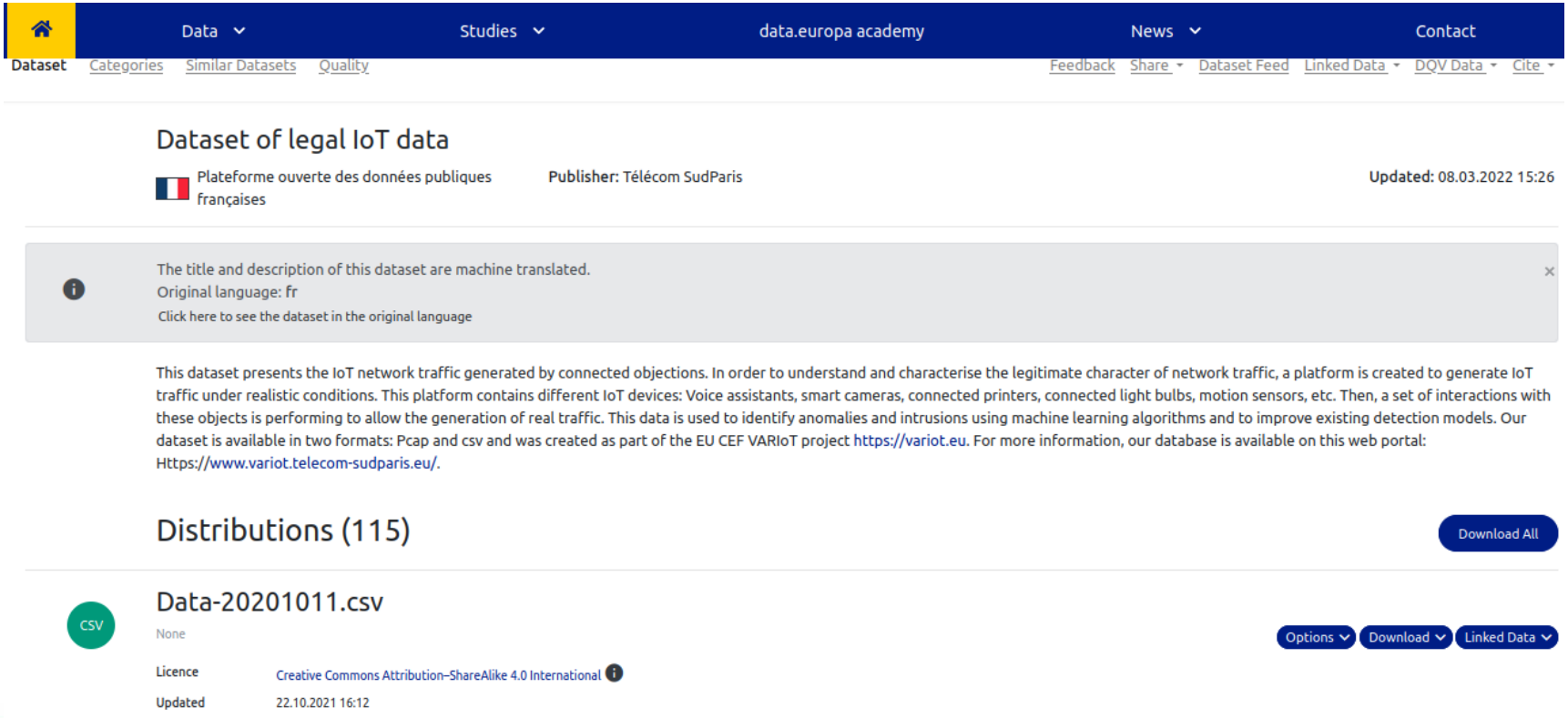
Co-financed by the Connecting Europe Facility of the European Union

- PIB, **NASK** (PL, coordinator)
- **Shadowserver** (NL)
- CIRCL, **SMILE** (LU)
- Télécom SudParis, **IMT** (FR)
- **MGEP**, Mondragon Unibertsitatea (ES)

## Objectives

- Create a DB covering **IoT vulnerabilities and exploits**
- Improve IoT-related data collection through **large-scale scanning**
- Create a DB of **heterogeneous information** related to IoT (IoCs, events, malware, etc.)
- Create datasets of both **legitimate** and **malicious IoT trafic**
- Create mechanisms of active **monitoring** and **harnessing** of IoT device information about *new types of threats*
- Create interfaces to **share data** (*EDP*, *MISP*, *Shadowserver*)


August-connect smart lock
Nest - Protect
Tp-Link - LB-120
Server
D-Link - DHC-S150
Philips - Hue Bridge
Access Point
Raspberry Pi 3 (DHCP server)
Nest - A0005
D-Link - DCS-8300LH
Tp-Link - HS110
Tecking - SP
Huawei - Honor 10 Lite
Google - Home
Tecking - SP

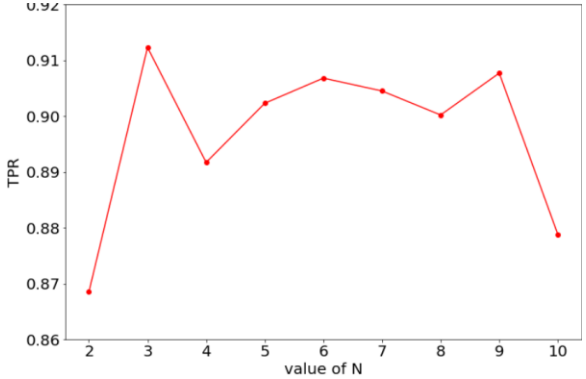

Data
Studies
data.europa academy
News
Contact
Dataset
Categories
Similar Datasets
Quality
Feedback
Share
Dataset Feed
Linked Data
DQV Data
Cite
Dataset of legal IoT data
Plateforme ouverte des données publiques françaises
Publisher: Télécom SudParis
Updated: 08.03.2022 15:26
The title and description of this dataset are machine translated.
Original language: fr
Click here to see the dataset in the original language
This dataset presents the IoT network traffic generated by connected objections. In order to understand and characterise the legitimate character of network traffic, a platform is created to generate IoT traffic under realistic conditions. This platform contains different IoT devices: Voice assistants, smart cameras, connected printers, connected light bulbs, motion sensors, etc. Then, a set of interactions with these objects is performing to allow the generation of real traffic. This data is used to identify anomalies and intrusions using machine learning algorithms and to improve existing detection models. Our dataset is available in two formats: Pcap and csv and was created as part of the EU CEF VARIoT project https://variot.eu. For more information, our database is available on this web portal: Https://www.variot.telecom-sudparis.eu/.
Distributions (115)
Download All
CSV
Data-20201011.csv
None
Options
Download
Linked Data
Licence
Creative Commons Attribution-ShareAlike 4.0 International
Updated
22.10.2021 16:12

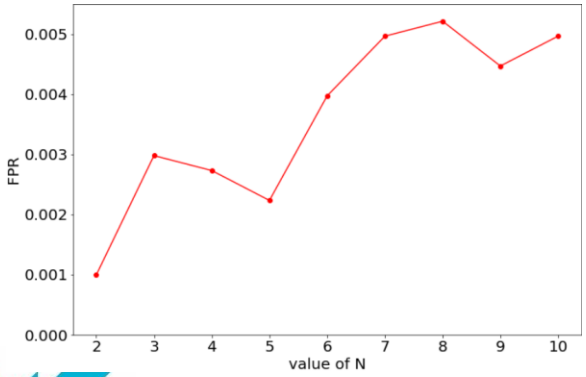
| Features |
|---|
| Mean, Median, Min, Max, Standard deviation and Count of the size of the first N packets sent |
| Mean, Median, Min, Max, Standard deviation and Count of the size of the first N packets received |
| Mean and Standard deviation of the IAT between the first N packets sent |
| Mean and Standard deviation of the IAT between the first N packets received |

| | Bidirectional flows |
|---|---|
| D-Link Motion Sensor | 1074 |
| Nest Security Camera | 1055 |
| TP-Link Smart Bulb | 1040 |
| TP-Link Smart Plug | 858 |
| **Total** | **4027** |

## IoT devices perform specific tasks

- Legacy monitoring systems are not expected to cope with the **increasing IoT traffic** volume
- Contrary to general-purpose IT systems, IoT devices perform very **specific tasks**
- We use *neural networks* to learn **legitimate IoT traffic behaviours**:
  - autoencoders reconstruct their inputs efficiently
  - one autoencoder is trained per device




## Tests on bidirectional TCP flows

- We focused on **TCP flows** of varying length N
- Training performed with *5-fold cross-validation*
- With a *modest subset* of our dataset, results seem *promising* but:
  - Performance is likely to *degrade* with the number of devices
  - Software updates incur *retraining*
  - A malware may learn to *mimic* such simple features

## Evaluating security measures

In particular, intrusion detection systems (IDS)

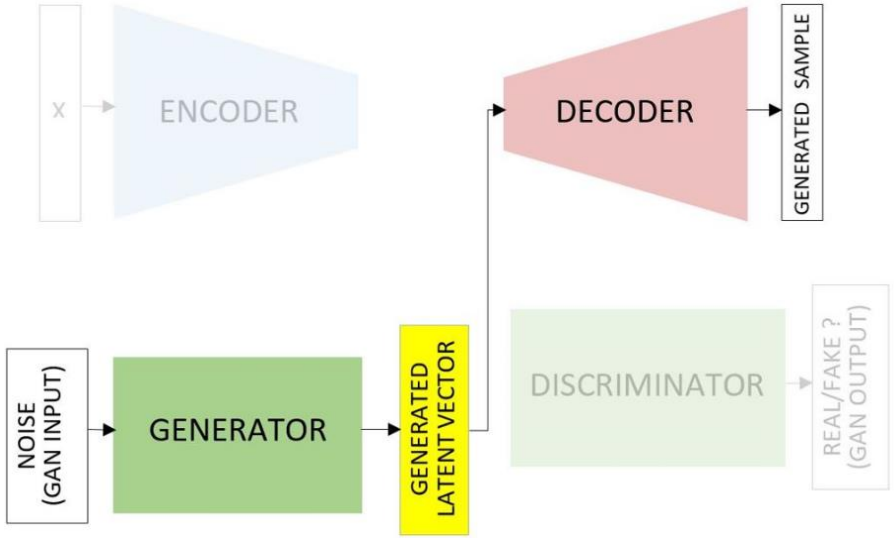
- Prior collaboration with DGA-MI on the topic of *evaluation testbeds*
- NIST's reference on IDS evaluation:
  - Anomaly-based IDS require **normal** traffic
  - Testing using normal traffic:
    - Replaying **real** traffic (*sensitive*, *unsound*)
    - Replaying **sanitized** traffic (*tedious*, *unsound*)
    - Generating traffic on a **testbed** (*costly*, *not scalable*)

## Synthetic traffic generation

**Objective-driven** generation of datasets

- *Proof-of-concept* by Ring et al. using a Generative Adversarial Network (GAN)
- Could be used for different evaluations:
  - Stress testing (*data augmentation*)
  - Adversarial testing
  - Evasion (Rigaki and Garcia)
  - Boundaries

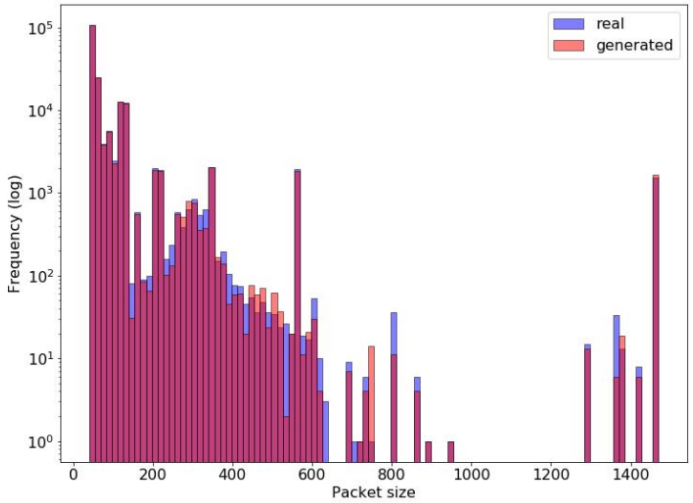
- Our objective was to **evade** *AI-based anomaly detectors* trained for smart IoT devices (e.g., voice assistants)




## Imitating an IoT device

We used a GAN to **generate similar** packet features

- GANs are *not successful* at generating sequence of categorical data
- *Inspired* from text generation by Donahue et Rumshisky:
  - an autoencoder (**AE**) is trained to learn sequences of packet sizes (*constructing a space of latent representations*)
  - a Wasserstein GAN (**WGAN**) is trained on the resulting latent space
  - at *generation time*, the GAN produces latent vectors, *decoded into realistic sequences* of packet sizes corresponding to bidirectional flows




| | OCSVM | IForest | EE |
|---|---|---|---|
| $FNR_{synthetic}$ (WGAN-GP) | .9817 | .9833 | .9047 |
| $FNR_{synthetic}$ (WGAN-C) | .9798 | .9886 | .8948 |
| $FNR_{test}$ | .0496 | .1053 | .0766 |
| TNR | .9762 | .9783 | .8754 |

## Synthetic samples less anomalous than real samples

- Compared different architectures with some VARIoT datasets (WGAN-GP, **WGAN-C**, VAE) using Earth mover's distance (EMD)
- Trained 3 anomaly detectors (OC-SVM, **IF**, EE) and *tested against mixed traffic* (0.9 < recall < 0.95)
  - Real voice assistant traffic
  - Compromised IoT traffic (IoTPot)
- Tested against synthetic samples only
  - Evasive samples are **better accepted** than real samples *due to legitimate outliers*

## Mimicry of a voice assistant

- Although **smarter** than most devices, we were *limited in the volume of interactions*
- **Extending** the problem space requires *additional (re)training*
- **Not flexible** with respect to bidirectional flow *ordering/alternation*
- **Limited** use case
  - exfiltration scenario (Rigaki and Garcia)
  - but could be applied to other compromised IoT scenarios such as *botnet*
- **Limited** applicability: *feature-space attack* but could be used for traffic morphing (Wright et al.)

## Feature- vs problem-space

- Features vectors ≠ traffic
- The inverse mapping problem (from feature vector to sample) is **not invertible** and **not differentiable** (Pierazzi and Pendlebury)
  - synthetic traffic *may not preserve* original traffic **semantics**
    - malware becomes goodware for real
  - still, we can use the resulting feature vectors *as input* to a traffic generator
    - see traffic generation demonstration

## Step 1: pcap generation

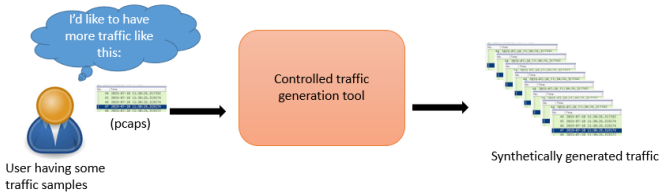
- Extract flow profiles from VARIoT pcap samples
  - packet size (min, max, mean, std)
  - IAT (min, max, mean, std)
- Compute β-distribution from the features and randomly sample values from it (500 packets)
- Generate pcap file using scapy

## Step 2: network replay

- Emulate network topology in ContainerNet (2 hosts & 2 switches and link delay of 100ms)
- Collect traces using tcpdump
- Replay pcap using tcpreplay

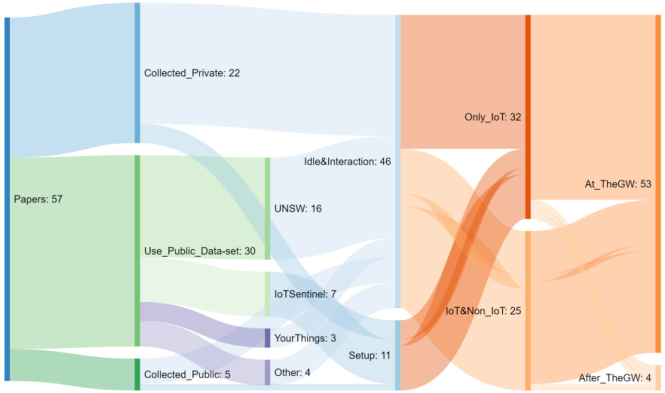
## Step 3: trace analysis

- Parse pcap file using tshark to extract the retained flow features (packet size, IAT)
- Compare extracted features with source profile
- Display the IAT distribution



## Scope

- **57** papers from 2017, **11** datasets
- Security (fingerprinting, scanning) and non-security (QoS, management) papers
- **Taxonomical** analysis
- *Submitted* to JNCA (Elsevier)




## Insights

- Proposed taxonomy: data processing (*from datasets to applications*)
- 3 classification levels (*category, type, instance*)
- 3 stream definitions (*pair of hosts, number of packets, time window*)
- Local traffic capture *favored* over external
- Datasets often *unbalanced, unlabeled, lack diversity, age quickly*
- No *scalable* feature extraction requirements

- Future avenues: scalability, transferability, industrialization

## VARIoT

- Run several traffic generation platforms (in Evry and Palaiseau)
- Collect radio-level communications (internal traffic)
- Generate malicious traffic (compromised IoT devices emulation)
  - Collaboration with **MGEP**

## GRIFIN

- ANR PRC project
- Continues exploiting VARIoT testbed
- Extends IoT testbed to emulate other IoT scenarios (e.g., IIoT, 5G)
- One Ph.D student working on distributed, adaptive anomaly detection and anomaly detection evaluation
- One vacant Ph.D position on *Cognitive and Programmable Response (vacant internship)*
  - more info at: https://anr-grifin.telecom-sudparis.eu/page/internships/

## Projects

- VARIoT: https://variot.eu
- GRIFIN: https://anr-grifin.telecom-sudparis.eu
- SPARTA: https://sparta.eu

## Figures


- G. Kambourakis et al.: *The Mirai Botnet and the IoT Zombie Armies*. In MILCOM'17. IEEE.
- Shadowserver: *Accessible CoAP Report – Exposed Constrained Application Protocol Service on the Internet*. 2020. URL: https://www.shadowserver.org/news/accessible-coap-report-scanning-for-exposed-constrained-application-protocol-services/
- VARIoT: *IoT Traffic Generation Sources*. 2019. URL: https://www.variot.eu/project-outcomes/iot-traffic/iot-traffic-generation-sources/


## Testbed, Datasets

- VARIoT IoT Legitimate Traffic Testbed: https://variot.telecom-sudparis.eu
- VARIoT Datasets of IoT Legitimate Traffic: https://www.data.gouv.fr/fr/datasets/dataset-of-legitimate-iot-data/
- IoTPot: Honeypot for Revealing IoT Cyber Threats: https://sec.ynu.codes/iot

## Publications


- M.R. Shahid et al.: *Anomalous Communications Detection in IoT Networks using Sparse Autoencoders*. In NCA'19. IEEE.
- M.R. Shahid et al.: *Generative Deep Learning for Internet of Things Network Traffic Generation*. In PRDC'20.
- H. Jmila et al.: *Smart Home IoT Device Classification using Machine Learning based Network Traffic Analysis: a Survey and Taxonomy*. In Journal of Network and Computer Applications. Elsevier (*submitted*).

## Citations


- D. Donahue and A. Rumshisky: Adversarial Text Generation without Reinforcement Learning. In arXiv preprint 1810.06640. arXiv, 2018.
- P. Mell et al.: *An Overview of Issues in Testing Intrusion Detection Systems*. NISTIR 7007. NIST, 2003.
- F. Pierazzi, F. Pendlebury et al.: *Intriguing Properties of Adversarial ML Attacks in the Problem Space*. In SP'20. IEEE.
- M. Rigaki and S. Garcia: *Bringing a GAN to a Knife-Fight: Adapting Malware Communication to Avoid Detection*. In SPW'08. IEEE.
- M. Ring et al.: *Flow-based Network Traffic Generation using Generative Adversarial Networks*. In Computers & Security 82. Elsevier, 2019.
- C.V. Wright et al.: *Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis*. In NDSS'09. ISOC.


## Tools

- ContainerNet: https://containernet.github.io/
- Scapy: https://scapy.net/
- tcpreplay: https://tcpreplay.appneta.com/
- Tshark: https://tshark.dev