



HAL
open science

VARIoT: vulnerability and attack repository for IoT

Gregory Blanc

► **To cite this version:**

Gregory Blanc. VARIoT: vulnerability and attack repository for IoT. RESSI 2020 - Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, Dec 2020, En ligne, France. hal-04165400

HAL Id: hal-04165400

<https://hal.science/hal-04165400v1>

Submitted on 24 Jul 2023

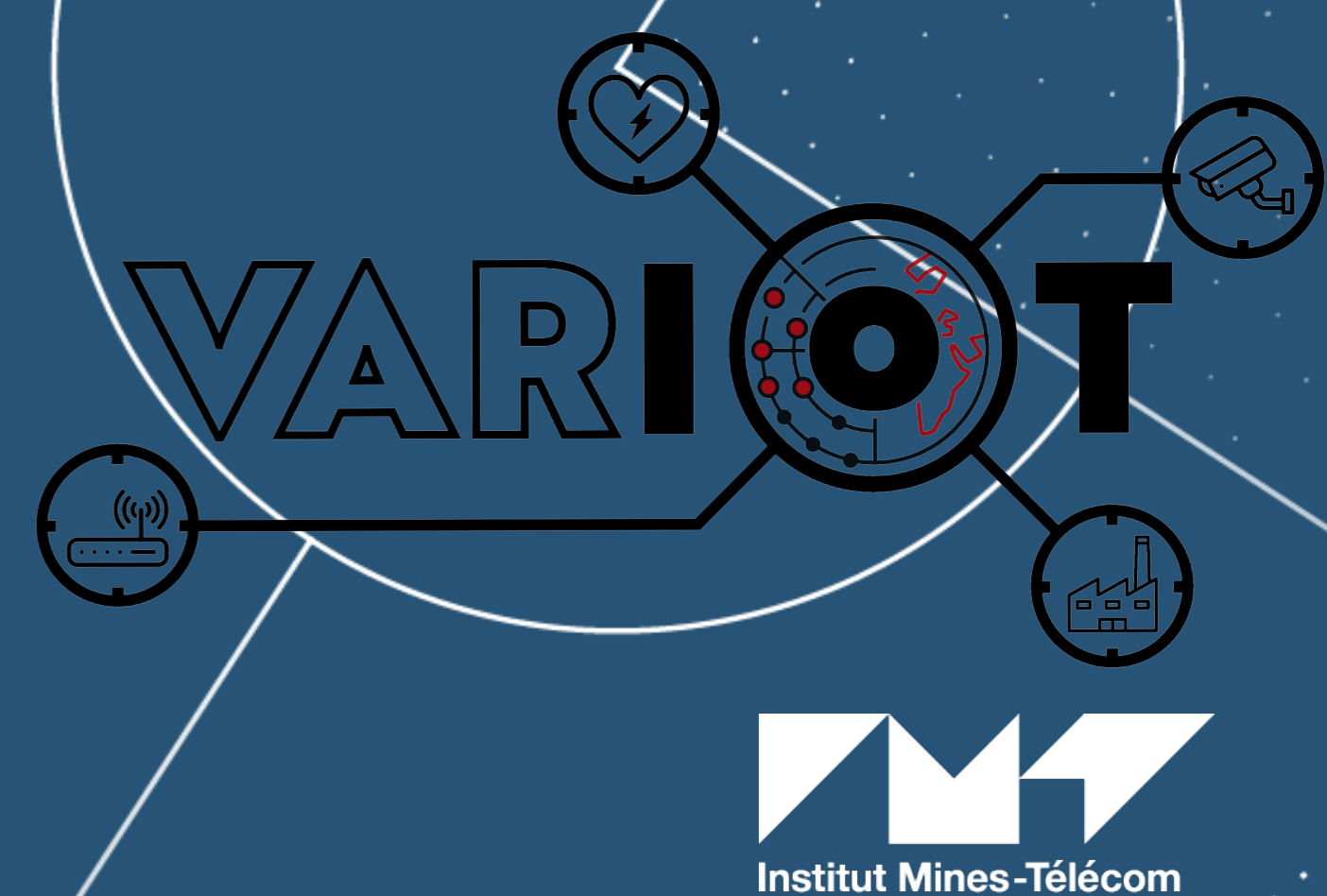
HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



CEF VARIOT

VULNERABILITY AND ATTACK REPOSITORY FOR IOT



Authors

Gregory Blanc
IMT/Télécom SudParis
Institut Polytechnique de Paris

Marek Janiszewski
NASK - PIB

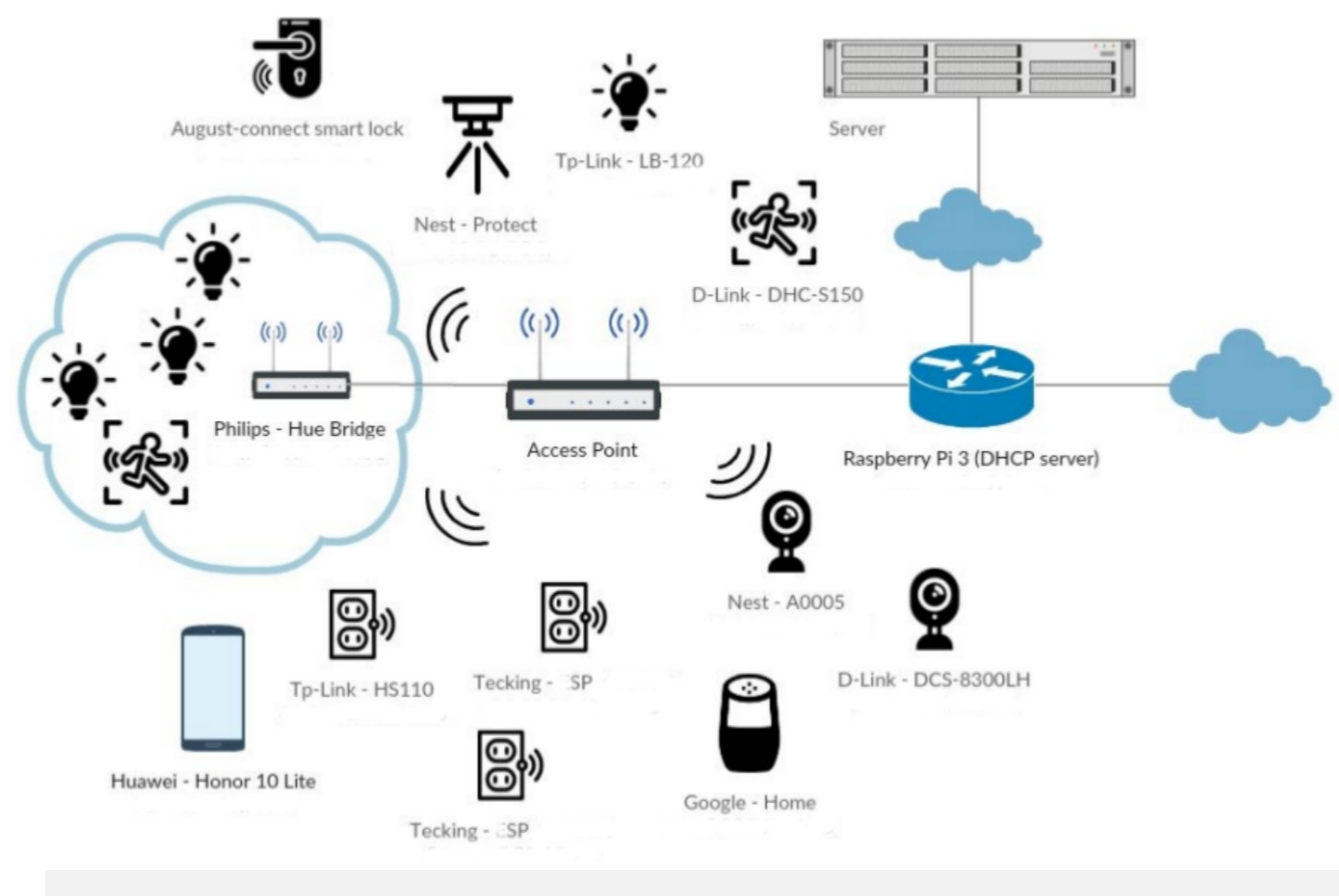
Piotr Kijewski
Shadowserver

Partners



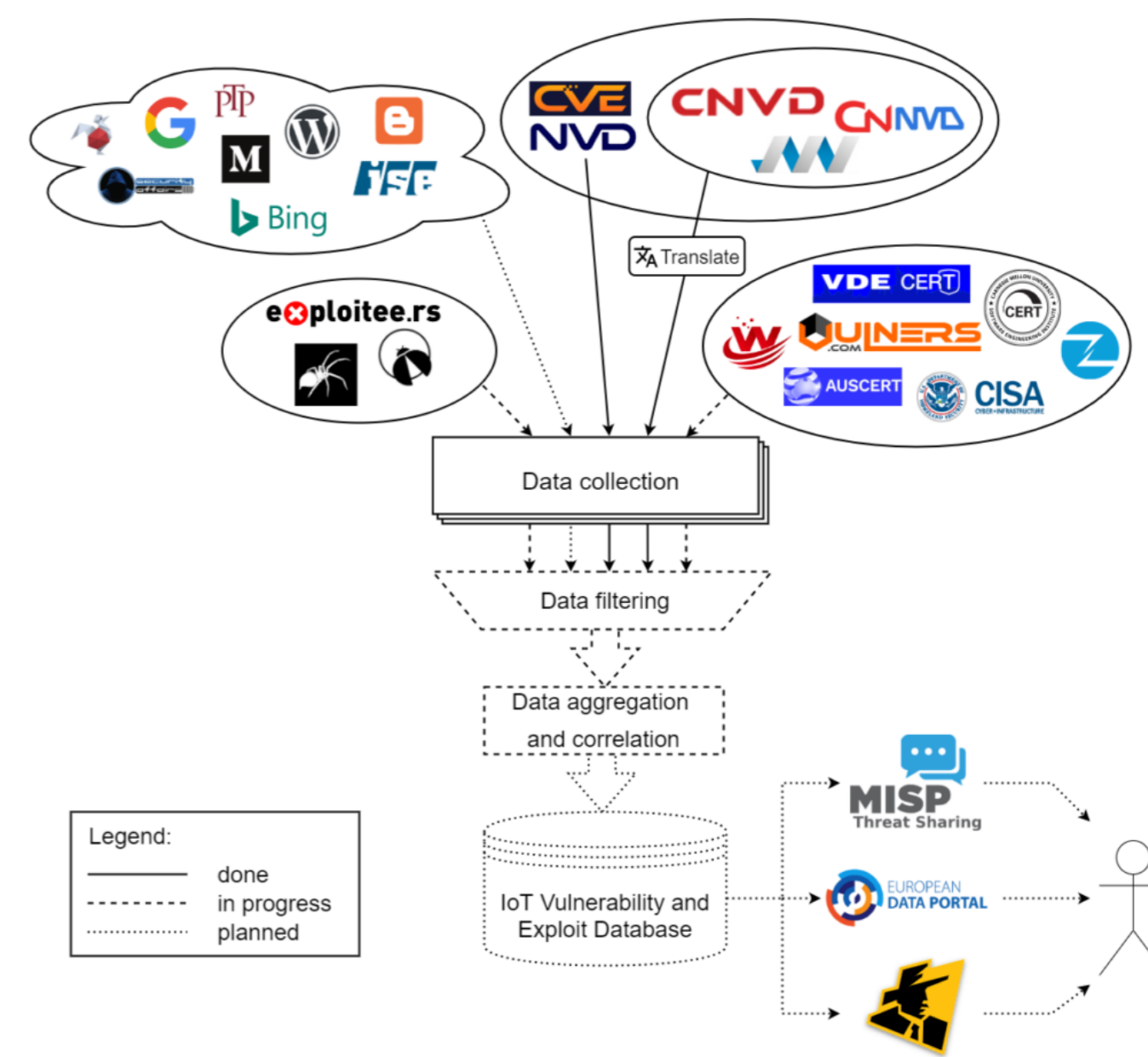
TRAFFIC GENERATION & MODELLING

- Network traffic analysis for IoT device identification: deep-learning-based solution for each device type, enabling anomaly detection
- IoT network traffic generation: setting up a testbed to generate real-life traffic daily
- Generate behavioural models for generalised anomaly detection: leverage previous results to transfer models learned in controlled environments to edge or user premises
- IoT malware analysis: understand compromised IoT behaviour, and generate malicious IoT traffic



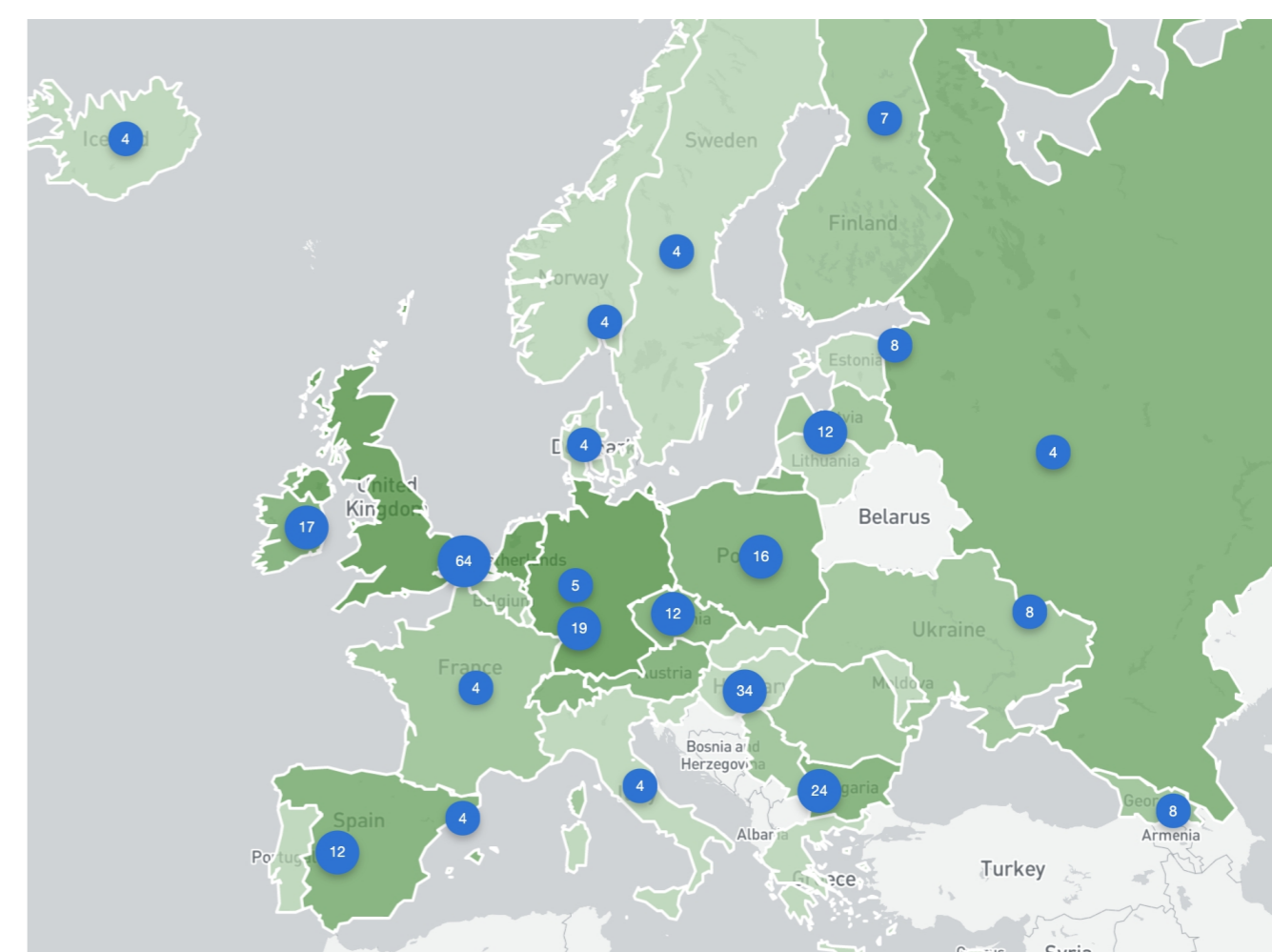
INTERNET-WIDE SCAN OF IOT PROTOCOLS

- Campaigns of Internet-wide (IPv4) scans for IoT-specific protocols: CoAP, MQTT, IPP
- Results shared daily with 114 national CSIRTs and 6000+ network owners worldwide
- Tagging scan results to enable IoT device identification (40M x509 certificates collected each day)
- Rule language developed for tagging: hundreds of rules currently being tested
- IoT-oriented honeypot network: 400 honeypots in 49 countries, 68 unique ASNs, and 202 /24 networks
- Future works include 1) scanning of IPv6 and new protocols; 2) development of a new honeypot type suited to observing IoT related exploits and malware



VULNERABILITIES & EXPLOIT DB

- Identification of data sources: vulnerability databases, security advisories, exploits databases, blogs, etc.
- Collection of data from the selected sources: parsing, and eventually translating sources' contents
- Filtering the data concerning IoT: requires device cataloguing to refine collected data
- Data aggregation, correlation and enhancement: creation of a common format to unify all sources; correlation of data for a single entry from different sources
- Publication of the data: European Data Portal, MISP Threat Sharing Platform, Shadowserver's free daily remediation feeds



View an X.509 rule

Details	Comments
Signature	= "Let's Encrypt Authority X3" and subject_common_name == /asuscomm.com/ and issuer_organization_name
Name	ASUS_asuscomm_lets_encrypt_cert_for_AiCloud
Description	This rule identifies ASUS routers by matching asuscomm in subject common name and lets encrypt - for AiCloud
Group	ASUS
Order	102
State	Testing

Data Sheet

CEF Telecom – Public Open Data

CEF-TC-2018-5

Started: July 1st, 2019

End: June 30th, 2022