Creating vulnerabilities and exploits database of IoT devices

Marek Janiszewski, Marcin Rytel, Piotr Lewandowski, Hubert Romanowski
Research and Academic Computer Network (NASK)
email: marek.janiszewski@nask.pl

Abstract

The poster presents outcomes of the process of creating a database that aggregates information about **vulnerabilities and exploits** regarding devices **of the Internet of Things**. The database was made under the **VARIoT (Vulnerability and Attack Repository for IoT)** project and is currently available online at **variotdbs.pl**. The aim of the database is to increase the level of security of IoT.

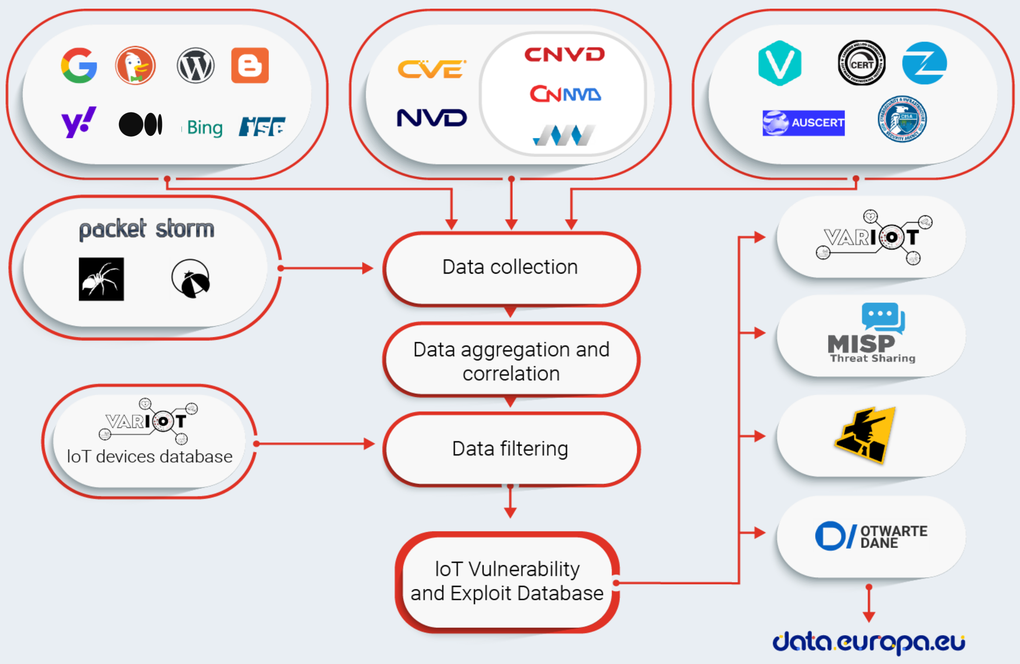
Reasons for creating the database

- lack of wide-known repository of such information dedicated to IoT
  - there are well-known databases of vulnerabilities (e.g. NVD) and exploits (exploit-db), they have a much wider scope than IoT, and they are not adjusted to the specificity of IoT
  - information about vulnerabilities and exploits are dispersed over many sources

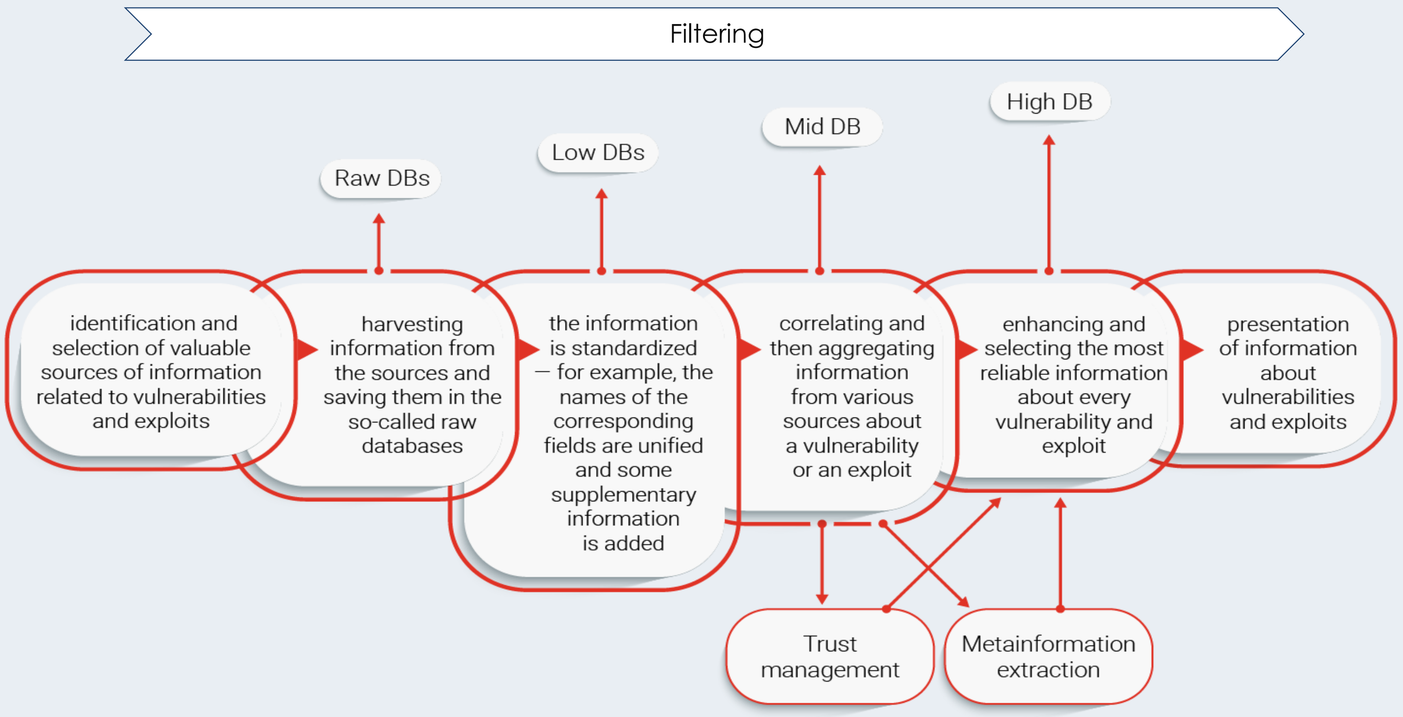
Requirements

- monitoring of information emerging in independent sources
- automatic harvesting and updating information
- storing historical information
- having rules of aggregation, correlation and conflict resolution
- ability of information enhancement, on the basis of:
  - extraction and classification of metainformation
  - trust evaluation

Database architecture



Approach and process of creation



Trust management

Trust evaluation is done to:

1. choose the most relevant information
2. present a trust score of created (correlated) information as a way of evaluating its reliability
3. identify vulnerabilities and exploits related to IoT

Trust evaluation is done on the basis of:

- reputation of the information source
  set on the basis of expert knowledge and historical quality of the source
- convergence of information from different sources
- method of aggregation and classification performed
- additional searches
- verification performed and changes introduced by analyst

Search engine

SEARCH ENGINE CONFIGURED TO GENERATE RESULTS ABOUT IOT VULNERABILITIES

- obtaining unstructured information about vulnerabulities of IoT devices from search engines, such as articles or blog entries

METAINFORMATION EXTRACTION AND GENERATING TRUST VALUE

spaCy NLTK

- extraction of metainformation from the obtained entries, using the information collected in the VARIoT database and NLP, ML/AI techniques
- defining trust value for obtained entry

Availability of the database

- it is possible to get the information both on the webpage and by the API
- data is also available in data.europa.eu (through the Poland's Open Data Portal) as well as in other sources such as the MISP platform (Malware Information Sharing Platform)

Contents of the database

Every entry in the database contains information about a single vulnerability or exploit.

The information includes, but is not limited to:

- title and description of the vulnerability or exploit
- severity level and CVSS (Common Vulnerability Scoring System)
- affected products
- identifiers from various databases
- level of trust related to every piece of information
- references
- information about patches and remediations

Our websites

https://variot.eu

https://variotdbs.pl

References

- M. Rytel, A. Felkner, and M. Janiszewski, "Towards a Safer Internet of Things—A Survey of IoT Vulnerability Data Sources," Sensors, vol. 20, no. 21, 2020. https://www.mdpi.com/1424-8220/20/21/5969
- M. Janiszewski, A. Felkner, P. Lewandowski, M. Rytel, and H. Romanowski, "Automatic actionable information processing and trust management towards safer internet of things," Sensors, vol. 21, no. 13, 2021. https://www.mdpi.com/1424- 8220/21/13/4359
- VARIoT - Vulnerability and Attack Repository for IoT. https://www.variot.eu/
- VARIoT IoT Vulnerabilities and Exploits Databases. https://www.variotdbs.pl/

Consortium

NASK, TELECOM SudParis, IP PARIS, SHADOWSERVER, Mondragon Unibertsitatea, CIRCL Computer Incident Response Center Luxembourg

Acknowledgments

Scientific work published as part of an international project co-financed by the Connecting Europe Facility of the European Union, TENtec n. 28263632 and by the program of the Minister of Science and Higher Education entitled "PMW" in the years 2020–2022; contract No. 5095/CEF/2020/2

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