VARIoT – Vulnerability and Attack Repository for the Internet of Things

Marek Janiszewski, Marcin Rytel, Piotr Lewandowski, **Hubert Romanowski**
Research and Academic Computer Network (NASK)
Email: hubert.romanowski@nask.pl

Abstract

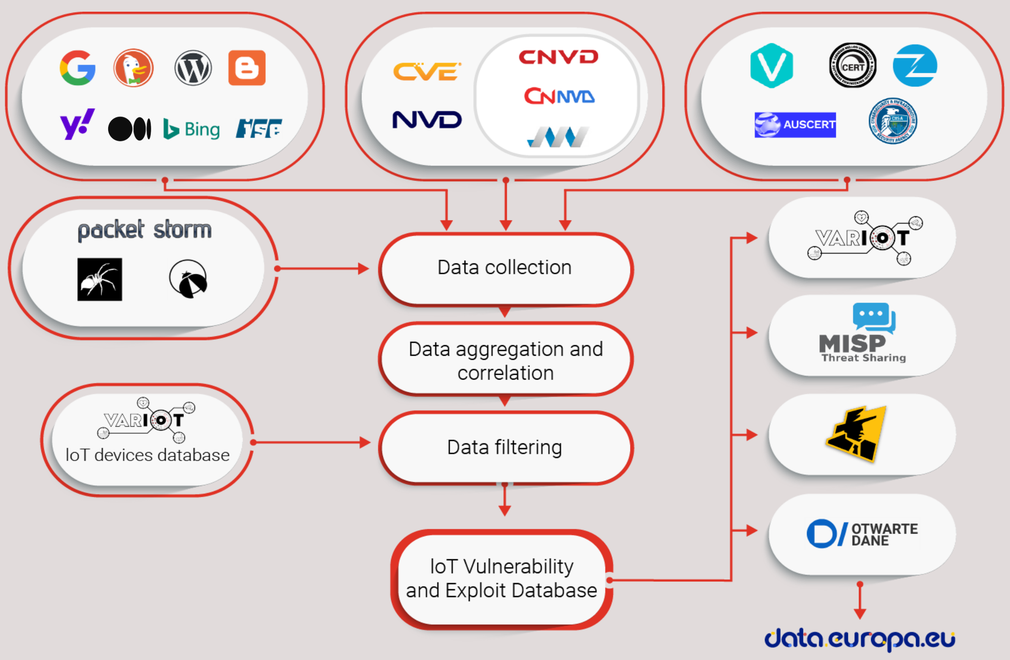
The security of the Internet of Things (IoT) has still not gained enough attention from researchers, developers and manufacturers, which results in exposing IoT users to possible threats. To make this situation a bit better, we have created, under the VARIoT (Vulnerability and Attack Repository for IoT) project, a database of information about vulnerabilities and exploits in the Internet of Things.

Introduction

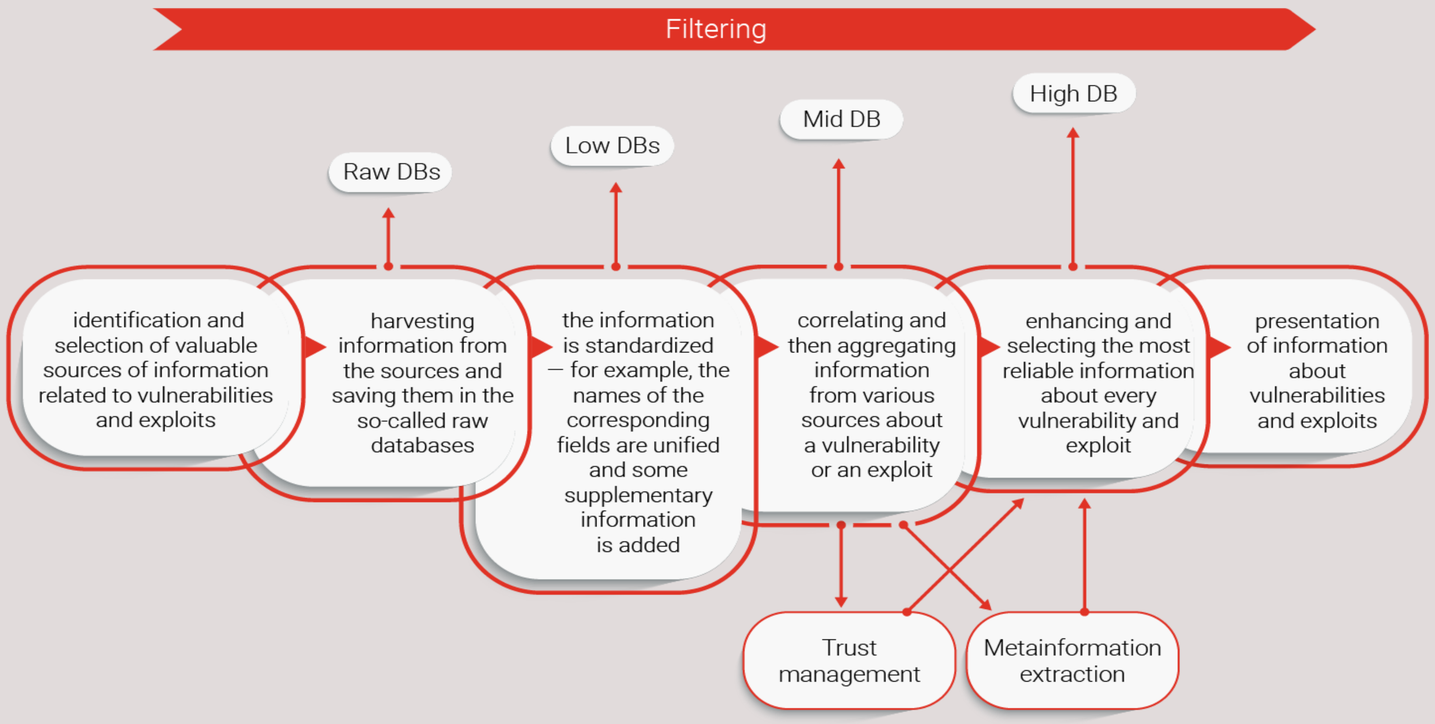
One of the main aims of the VARIoT (Vulnerability and Attack Repository for IoT) project was to create vulnerabilities and exploits database dedicated to the Internet of Things, which will be constantly updated by harvesting various sources of information publicly available on the Internet. All these actions are important for various types of stakeholders, such as:

- CSIRTs (Computer Security Incident Response Teams)
- device producers and users
- Internet service providers, network owners

Sources of information



Approach and process of creation



Trust management and metainformation extraction

To extract specific information from the block of text we have:

- used various artificial intelligence and natural language processing mechanisms
- prepared dictionaries containing information about vendors, models, device types and vulnerability types. Such dictionaries were used in two ways: as keywords to be searched in text and as training datasets for other methods.

The process of evaluation of trust to information takes into account various factors:

- the reputation of each source estimated on the basis of its reliability
- general accuracy and comprehensiveness of information presented in the source
- recognition of the source in community
- documentation about the source
- stability and the uniqueness of information provided as well as self-consistency of information within the source.
- consistency with information from other sources is also taken into account during trust estimation

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) score
- affected products
- identifiers from external databases
- level of trust related to every piece of information
- references
- information about patches and remediations

Availability of the database

- It is possible to get the information both on the webpage and by API
- Data will be available also in data.europa.eu Portal (through the Poland's Open Data Portal) as well as in other sources such as MISP (Malware Information Sharing Platform), which is commonly used by the community of cybersecurity analysts

Our websites

https://variot.eu

https://variotdbs.pl

Acknowledgment

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

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, p. 5969, oct 2020. [Online]. Available: 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. [Online]. Available: https://www.mdpi.com/1424- 8220/21/13/4359

Consortium

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

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

and by the program of the Minister of Science and Higher Education entitled "PMW" in the years 2020-2022