Community Based Platform for Vulnerability Categorization

Jana Komárková*†, Lukáš Sadlek*†, Martin Laštovička*†
*Institute of Computer Science, †Faculty of Informatics
Masaryk University, Brno, Czech Republic
{komarkova, lastovicka}@ics.muni.cz, sadlek@mail.muni.cz

***Abstract*—Many approaches, such as attack graphs, require knowledge of vulnerability's properties such as impact, prerequisities, and exploitability. Currently, those properties are either categorized manually or too roughly. We present a program for granular, automated categorization of vulnerability. Further, we present a platform supporting researchers by gathering and sharing raw data about vulnerabilities and community labeled datasets. The source code of our categorization program is available on GitHub.**

I. Introduction

Lot of approaches for attack prediction, attack correlation or vulnerability patching requires knowledge of vulnerability properties [1], [2], [3]. Such properties include vulnerability exploit prerequisities, impact of exploiting a vulnerability and, should we want to introduce probabilistic treatment, likelihood of successful exploit.

So far all this information has been taken from manually analyzed data or from the semi-formalized rough categorization provided by National Vulnerability Database (NVD). However, the sheer amount of disclosed vulnerabilities precludes the manual categorization as witnessed by closure of Open Sourced Vulnerability Database in 2016.

Our solution gathers the publicly available information about vulnerabilities and provides both categorized data and data sources for further research of vulnerabilities' properties.

II. Vulnerability Information Sources

In this section, we describe sources of information on vulnerabilities used for vulnerability categorization.

The National Vulnerability Database (NVD) [1] is a cyber security vulnerability database maintained by the National Institute of Standards and Technology (NIST) Computer Security Division. NVD provides a description of each vulnerability as well as a Common Vulnerability Scoring System (CVSS) score.

CVSS score is a structured description of the principal characteristics of the vulnerability[2]. The latest version of the CVSSv3 has been used since 2016. All vulnerabilities (including the latest one) are scored using CVSSv2.

Another publicly available source which will be included in our platform is vendor provided information. Each vendor provides (mostly unstructured) information about vulnerabilities in his products. Since the vendors are the most credible source, such information can be valuable.

[1]https://nvd.nist.gov/
[2]https://www.first.org/cvss/

978-1-5386-3416-5/18/$31.00

III. Vulnerability Description

We identified three main properties that could researchers find useful: impact, prerequisities of vulnerability exploit, and probability of successful exploit.

A. Impact

For the purpose of attack graph building, we have created following categories of vulnerability exploit impact:

- arbitrary code execution as root/administrator/system,
- gain root/system/administrator privileges on system,
- privilege escalation on system,
- gain user privileges on system,
- arbitrary code execution as user of application,
- gain privileges on application,
- system integrity/availability/confidentiality loss,
- application integrity/availability/confidentiality loss,
- communication integrity/availability/confidentiality loss.

The categories are not exclusive, vulnerability can have multiple impacts on system. The categories were designed to follow the rough categorization in NVD. Granularity was added in order to more accurately model the reality. Each category captures either a attacker's privilege gain or attacker's capability to command or harm the target.

B. Prerequisities

The prerequisities are sufficiently categorized in CVSS by attack/access vector (CVSSv2/CVSSv2) and privileges required (CVSSv3).

C. Likelihood of Exploit

The probability of successful exploit are covered in CVSS in attack/access complexity (CVSSv2/CVSSv2), user interaction (CVSSv3) and exploitability (CVSSv2).

IV. Vulnerability Impact Categorization

In this section we present a proof-of-concept program for vulnerability impact categorization. The program uses CVSSv2, CVSSv3, CPE and text description to derive the impact. It utilizes a differences between CVSSv2 and CVSSv3 methodologies, namely that the CVSSv3 impact is related

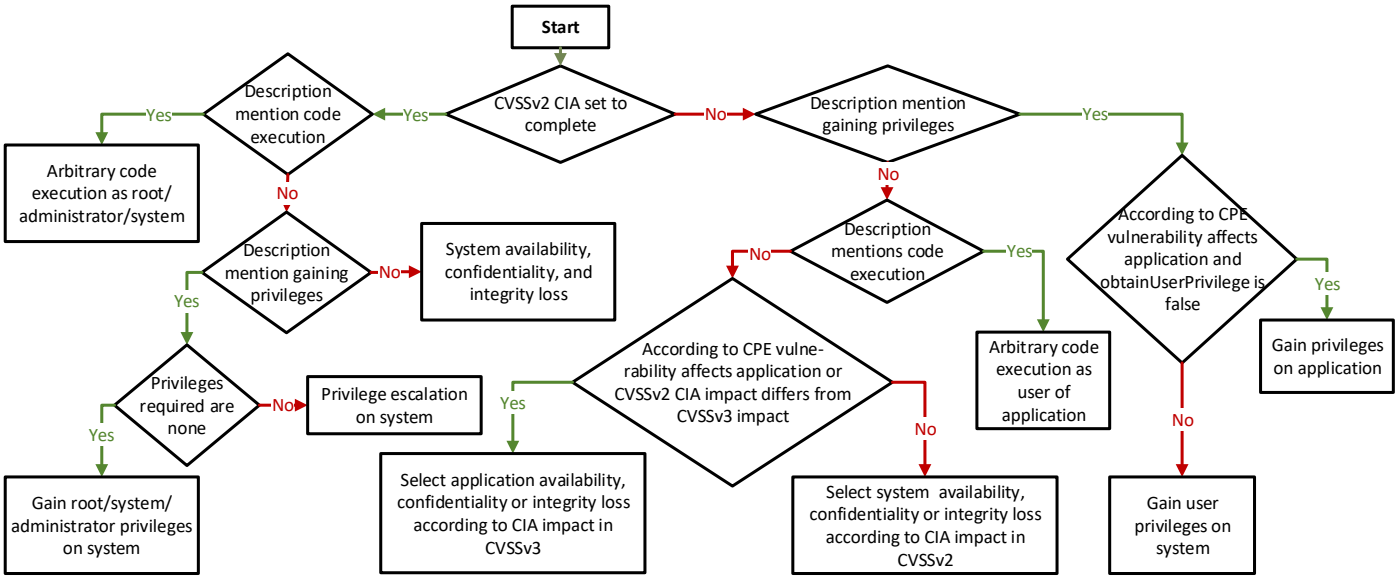

Fig. 1. Vulnerability impact categorization chart.

to the actual source of the vulnerability (i.e. OS, software) and CVSSv2 impact is related to the whole system. The approximate decision chart of the algorithm is shown in Figure 1. The source code of the program is available on GitHub[3].

V. Demonstration of Crowd-sourced Platform for Vulnerability Categorization

In the demonstration of the crowd-sourced platform for vulnerability categorization, we will present its following features:

1) Vulnerability Information - the first, most simple feature is the accumulated raw information about vulnerability gathered from various publicly available sources mentioned in Section II. The information will be sorted by CVE id.
2) Categorized Vulnerabilities - further, each vulnerability is categorized and the results are available for everyone in machine readable format.
3) Feedback - the platform enables the community to rate the accuracy of categorized information, thus providing both measure of efficiency of used approach and extends the categorized data by indication of the correctness (per vulnerability).
4) Labeled Data - the feedback is also used for creation of dataset with labeled vulnerabilities, which will be provided for general usage. This will help development of more accurate categorization methods.

The first version of the platform is available at https://crusoe.ics.muni.cz/vulnerability.

[3]https://github.com/CSIRT-MU/VulnerabilityCategorization

VI. Conclusion

Our community sourced platform for vulnerability categorization supports researches by providing automated formalized vulnerability description. Further, the platform allows the community to rate the results and therefore facilitates the evaluation of the vulnerability categorization program. Moreover, the labeled samples will be made into datasets, thus supporting development of more efficient methods for categorization.

In future work, we plan to develop more sophisticated methods based on the gathered information and add more information from other sources. We hope that, in time, our platform will help the researchers with accurate and granular data about vulnerabilities.

Acknowledgements

This research was supported by the Security Research Programme of the Czech Republic 2015 - 2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20172020070 Research of Tools for Cyber Situational Awareness and Decision Support of CSIRT Teams in Protection of Critical Infrastructure.

Martin Laštovička is Brno Ph.D. Talent Scholarship Holder – Funded by the Brno City Municipality.

References

[1] S. Jajodia, S. Noel, P. Kalapa, M. Albanese, and J. Williams, "Cauldron mission-centric cyber situational awareness with defense in depth," in *Military Communications Conference, 2011-MILCOM 2011*. IEEE, 2011, pp. 1339–1344.

[2] X. Ou, S. Govindavajhala, and A. W. Appel, "Mulval: A logic-based network security analyzer." in *USENIX Security Symposium*. Baltimore, MD, 2005, pp. 8–8.

[3] J. Xiao and J. Rofrano, "Managing vulnerabilities in a cloud native world with bluefix," in *Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on*. IEEE, 2017, pp. 726–740.