CrawVulns - A Software Solution for Vulnerabilities Analysis

Alin ZAMFIROIU[1,2], Paul POCATILU[1], Sergiu CAPISIZU[3]
[1]Bucharest University of Economic Studies, Romania
[2]National Institute for Research and Development in Informatics
[3]Bucharest BAR Association
alin.zamfiroiu@csie.ase.ro, ppaul@ase.ro, sergiu.capisizu@yahoo.com

Mobile devices and applications are very popular worldwide. Android and iOS dominate the mobile operating systems market. Most of the mobile applications connect to external servers that process and store users' data. These systems are exposed to malicious attacks and the developers should be always concerned about the applications and data security. This paper presents known threats and vulnerabilities related to mobile applications and proposes a software solution for vulnerabilities analyses (CrawVulns) that aims to help eliminate or mitigate security risks.

***Keywords**: Common Vulnerabilities and Exposures (CVEs), Mobile, Data, Security, Vulnerability.*
DOI: 10.24818/issn14531305/24.1.2020.04

1 Introduction

Almost all mobile applications use cloud storage because it saves data on your mobile device, reduce cost, and provide reliability and support disaster recovery [1], [2]. These data have to be protected against the unauthorized access. Security for mobile devices and for mobile applications is provided in different areas of interest such as:

- authentication, with verification of virtual identity, by requesting personal authentication information and verifying them with previously provided information at the time of registration. According to [3] authentication is the process by which the correctness and truthfulness of the information relating to the identity or origin of an entity is established or confirmed.
- communication or text messaging is one of the core business of mobile devices as well as transactions. This is a very important segment where security is vital to protect mobile device users. In [4] the SMSEncrypt application for people who want secure communication via the SMS service provided by the mobile phone company is presented. The SMSEncrypt software is composed of two modules: a module for sending encrypted messages with the specified key and the second module for receiving messages and decryption with the secret key the message receiver needs to know.
- the information is stored in the cloud as a backup for mobile device destruction; In the device's internal memory, the user stores photos taken with this device, text messages used to communicate with others, emails saved in the phone's memory, other people's contacts, or contact list; all this information in case of damage to or destruction of the mobile device is lost and its recovery is impossible or very difficult; it is recommended that you keep a backup in the cloud [5];
- encrypting the information stored locally for the case when the device is lost or stolen by others, so personal information is at their disposal; so the information that the previous recommendation is saved in a cloud backup is stored on the device but protected by a password, access to which is only allowed by specifying the encryption key.

In all these areas, security should be assured for the user data through the mobile application, because the data is used in various contexts.

This paper extends previous research from [14] and it is structured as follows. The next section presents the related work in this field.

The paper continues with an analysis related to Common Vulnerabilities and Exposures of mobile data. The next section presents the proposed solution. The last section is dedicated to countermeasures from two perspectives: hardware and software. The paper ends with conclusions and future work.

2 Related Work

According to [6], there are different types of security threats for mobile applications. These include application-based, Web-based threats, networks, but also physical threats.

Application-based hazards happen when users install applications from non-trust sources that look legitimate but actually these applications open backdoors from the device and share data and information from their device, without people realizing this thing.

Web-based threats is really frequent nowadays because anybody is using the mobile device to navigate on internet. This threat appears when users visit, in the mobile device' browser, infected sites that look harmless on the front end, but in reality, these websites automatically download malicious content or malicious applications to devices. These applications will start automatically even without the knowledge of the users.

Network-based threats appear when the users are using public WiFi networks from the airports or restaurants. In these public networks anybody can access the information from their devices or can leave some malicious applications on the device that can steal information. The real threat in this situation is that the network can be affected or tracked and all data and information will be accessed also by somebody else like the man-in-the-middle (MITM) attacker. Figure 1 depicts this situation.

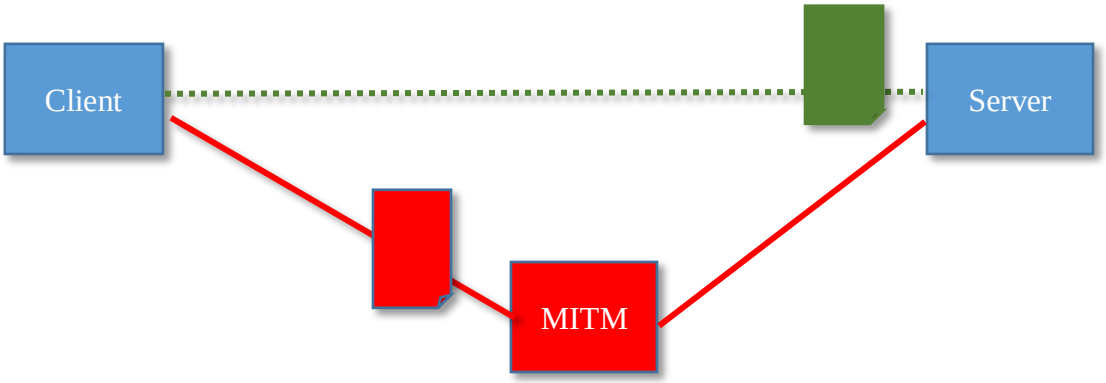

Fig. 1. Network-based threats

The *physical threats* occur when the mobile devices are stolen or the users loses them. In this way the unauthorized persons will access these devices and also the data and information from these devices.

Even if more and more articles exist in the direction to protect the mobile devices and to increase the security level of them, it is surprising to find that a big number of mobile users do not use a password or any other type of protection to lock their phone.

Also exists a big number of users that create PINs or passwords very easy to remember such as "0000" or "1234". These passwords are easy to remember but at the same time easy to identify by malicious people.

In their paper, Altuwaijri and Ghouzali [7] presented a threat model for storing mobile device data of Android based devices. Their model classify threats into physical and software threats. Physical threats are possible when mobile devices get into the hands of unauthorized people through loss or theft. The types of physical threats are [7]:

- *Cold boot attack* – assumes that ram memory is obtained and connected to another device to obtain data from that memory;

- *Evil maid attack* – assumes the unencrypted memory area; even if a password is used to encrypt data on your mobile device, the Android partitioning system can be modified with keylogging;
- *RowHammer* attack – assumes the use of management vulnerability at the lower levels of the operating system; is the most complex vulnerability of physical.

Software threats include malware attacks or poor mobile application development [7], [8] and they are falling in the following categories:

- *Malware attack* – involves installing applications that contain malware, which then develops into the infected mobile device;
- *Poor app development* – in this category, developers' level of knowledge of security concepts and how they develop mobile applications; if developers do not implement community-approved security standards, the developed application will be very vulnerable in terms of security.
- *Attacks based on device public information* – involves knowledge of mobile devices and applications running on these devices, and attackers use these vulnerabilities to perform attacks;
- *Routing* the device to remove limitations imposed by the developer leads inevitably to the emergence of new vulnerabilities that can be exploited by attackers.

OWASP, the non-profit group that helps companies develop and service security applications issued in 2016 a document with the most used vulnerabilities for mobile applications [9]. These are shown in Figure 2.

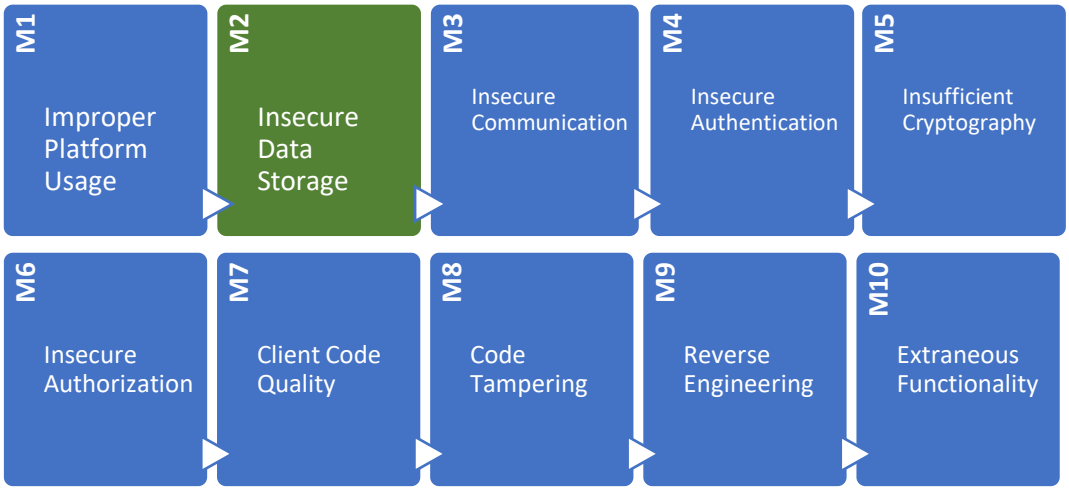

Fig. 2. OWASP Mobile Top 10 Risks [9]

For each vulnerability, the ways to check if mobile applications are vulnerable and how to prevent these vulnerabilities.

3 Common Vulnerabilities and Exposures of Mobile Data

Common Vulnerabilities and Exposures [10] provide a reference method for publicly known vulnerabilities and exposures. Within the CVE vulnerability base are stored all the important IT vulnerabilities discovered so far. Shortly after a new vulnerability is discovered, it is documented and receives a new unique identifier in the CVE list. Currently, the CVE vulnerability base is a reference source for cyber security specialists.

In order to select only CVEs relevant to mobile app data, in this paper, we started with a list of mobile-specific keywords and used them to search for the common **vulnerabilities**. As mobile devices as well as mobile applications have a rapid increase but also a high degree of change, CVEs are selected in the last three years: 2017, 2018 and 2019.

Table 1 lists CVEs relevant to mobile application data, grouped by key terms used for search.

Table 1. CVEs specific for mobile data

No.	Keyword	Number of CVEs found (2017-2019)	Total number of CVEs found
1	mobile applications	16	27
2	mobile data	39	89
3	sensitive data	363	1088
4	Android data	196	409
5	phone data	10	24
6	iOS data	40	127
7	device data	117	242

For the 7 terms used, 2006 CVEs were identified, out of which 781 were documented in the last years, 2017-2019. For the term "sensitive data", most CVEs have been identified, as is also shown in Figure 3.

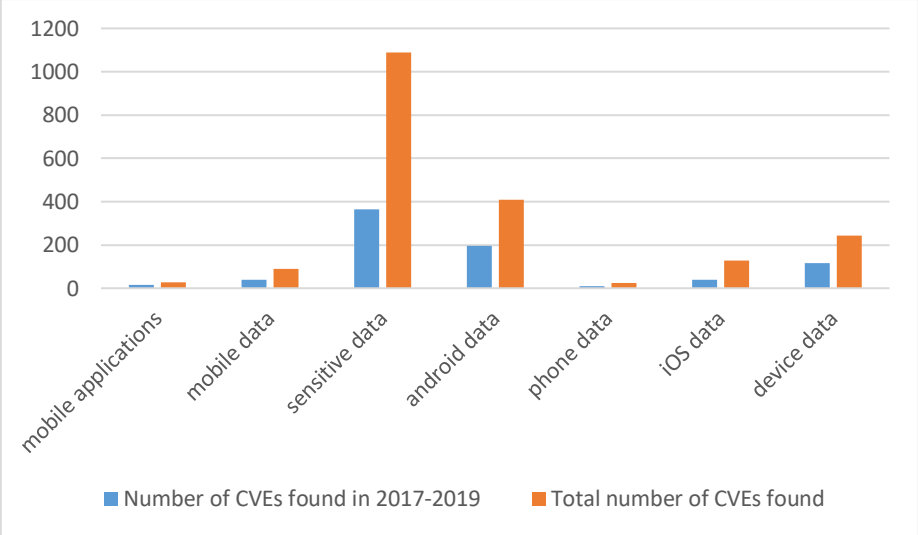

Fig. 3. Identified CVEs for Mobile Data

Of the 781 CVEs identified between 2017 and 2019, 107 fall into two or more categories. Table 2 lists CVEs that are found in three or four categories. To identify the common vulnerabilities for all categories we used a word counter as in [11].

Table 2. Common Vulnerabilities per categories

No.	CVE	Number of categories	Categories
1	cve-2018-4844	4	mobile data, Android data, iOS data, device data
2	cve-2018-6599	4	sensitive data, Android data, phone data, device data
3	cve-2018-4847	4	mobile data, sensitive data, iOS data, device data
4	cve-2018-14995	4	sensitive data, Android data, phone data, device data
5	cve-2017-18125	3	mobile applications, mobile data, Android data
6	cve-2017-10188	3	mobile applications, mobile data, Android data
7	cve-2017-12228	3	sensitive data, iOS data, device data
8	cve-2018-14984	3	Android data, phone data, device data

No.	CVE	Number of categories	Categories
9	cve-2017-10132	3	mobile applications, mobile data, iOS data
10	cve-2018-14985	3	mobile data, Android data, device data
11	cve-2018-15005	3	mobile data, Android data, device data
12	cve-2018-14987	3	mobile data, Android data, device data
13	cve-2018-0461	3	sensitive data, phone data, device data
14	cve-2017-17225	3	mobile data, phone data, device data
15	cve-2018-4168	3	sensitive data, iOS data, device data

Thus, out of the 781 CVEs, the unique ones are 655. Figure 4 shows the relationships between the category vulnerabilities: {device data, mobile data, iOS data, mobile applications}.

Only these five categories were chosen because the other two {Android data, sensitive data} contain many elements and the visibility would not have been of any quality.

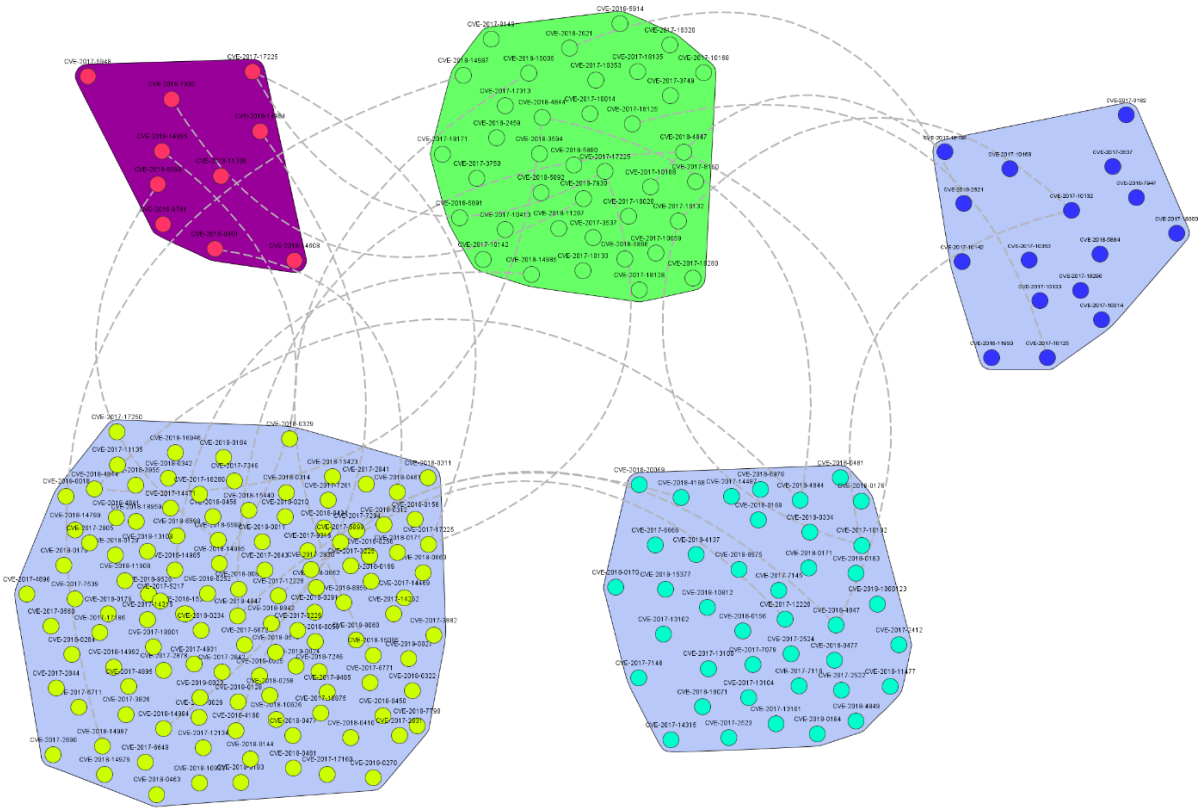

Fig. 4. The links between the vulnerabilities of the categories

The list of CVEs is updated daily, so there are certainly more vulnerabilities for data used in mobile applications.

4 Automated Tool for Vulnerabilities Analysis

In order to easily perform these analyses on existing vulnerabilities, a solution was developed. CrawVulns application was written in C# programming language and it is based on .NET technologies. The CrawVulns application works as a crawler, and for certain key phrases provided by the user, all vulnerabilities reported in the cve.mitre.org platform are searched, Figure 5.

.

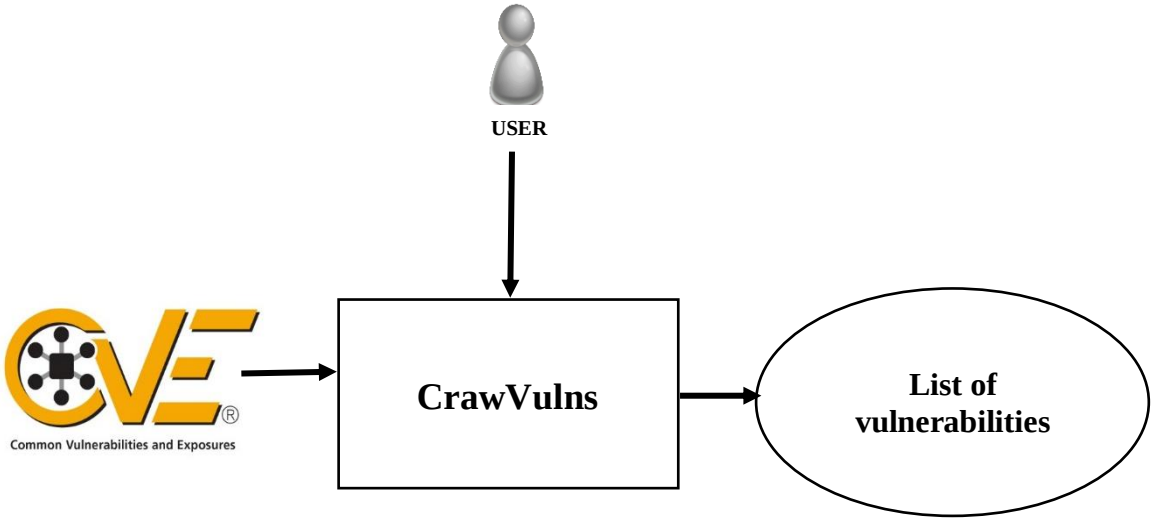

Fig. 5. Structure of the first module of CrawVulns application

The user will enter the keywords to generate the groups to identify the vulnerabilities.
The next step in the implementation of the CrawVulns is that with the obtained list of vulnerabilities, the CrawVulns application will connect to the nvd.nist.gov to obtain the base score impact for each identified vulnerability, Figure 6.

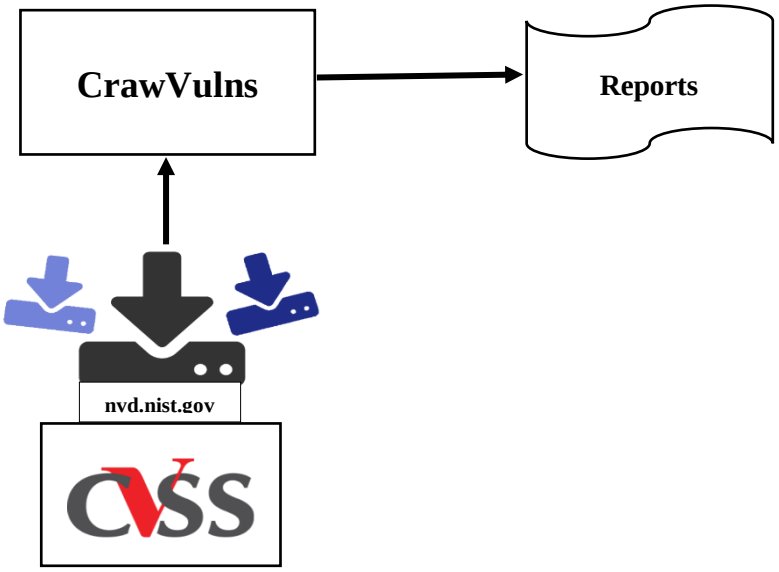

Fig. 6. Structure of the second module of CrawVulns application

In this way, we will obtain very easy the impact of each vulnerability for some keywords and we can create different reports for our analyses.

For the analysis made in the previous section with the CrawVulns application the results are presented in Figure 7.

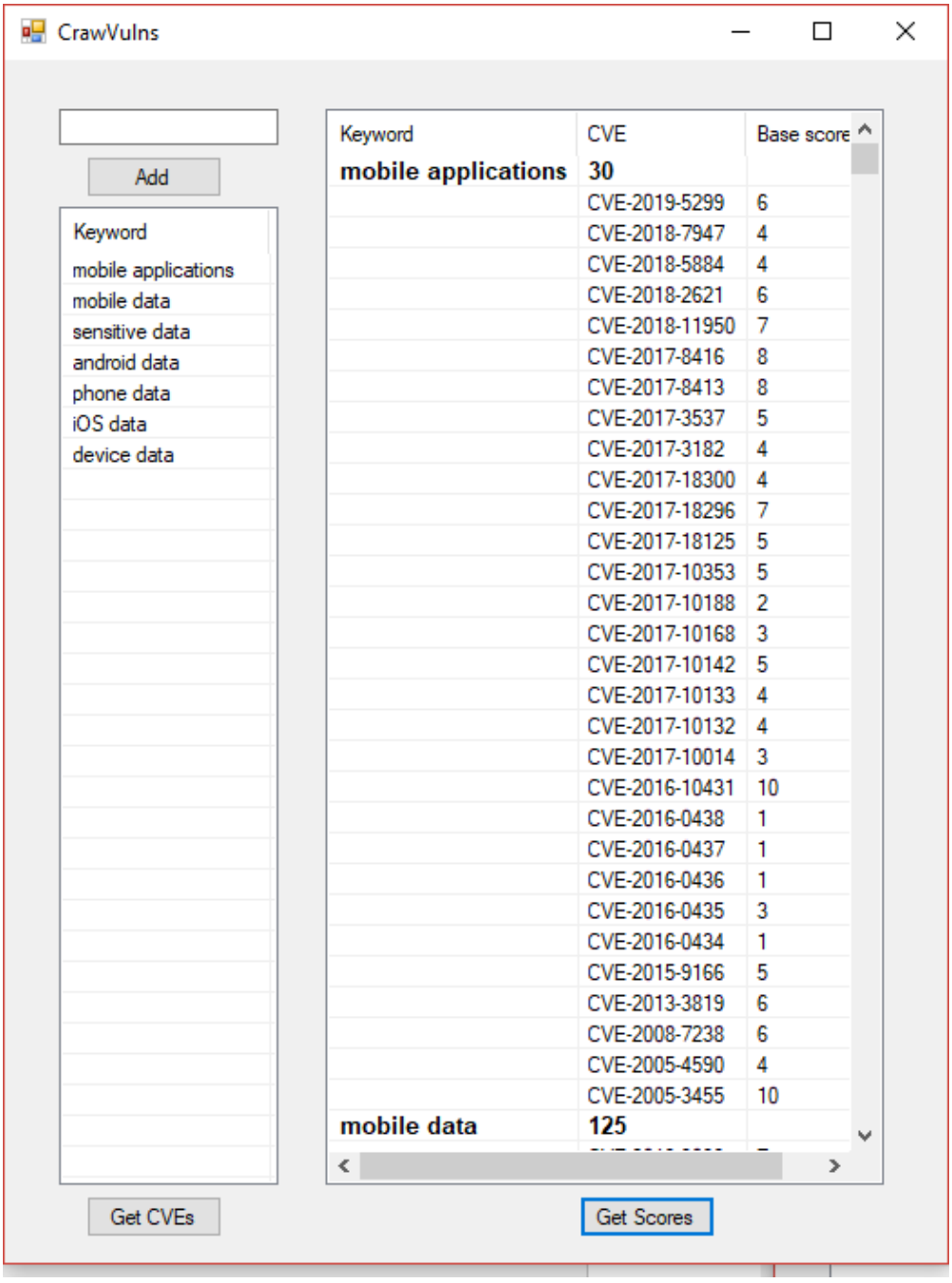

Fig. 7. CrawVulns application

The score is calculated by the following formula [13]:

$$ISC = 6.42 * (1 - (1 - I_C) * (1 - I_I) * (1 - I_A))$$

where:
I_C – Confidentiality impact;
I_I – Integrity Impact;
I_A – Availability impact.
These values are specified by the user on the platform, Figure 8.

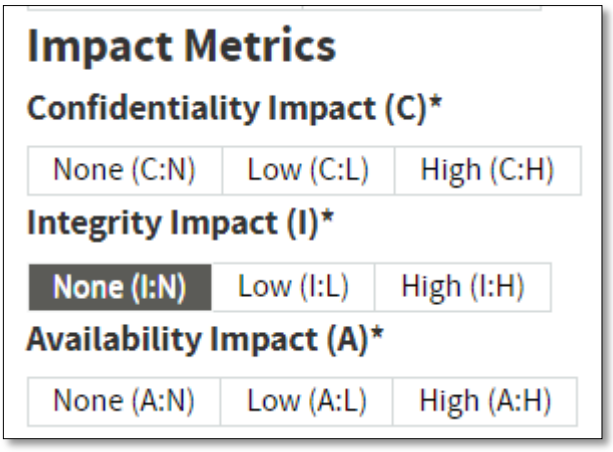

Fig. 8. Impact metrics on the NVD platform [13]

With these scores we can calculate the average of the impact for each solution.
Using the CrawVulns we can analyze the impact of CVEs of more domains and more solution used in these fields.

5 Threats countermeasures

Software developers and users have to take into account several countermeasures in order to avoid or mitigate the threats. In literature, countermeasures have been identified for vulnerabilities in the wild, as well as for vulnerabilities found for data used in mobile applications. There are two perspectives related to these countermeasures: hardware and software. In [7] there are some solutions for mobile devices running Android OS. These are presented in Table 3.

Table 3. Hardware solutions for data security on mobile devices [7]

No.	Solution	Implemented by:
1	CleanOS	Xia Y., Liu Y., Ma m., Guan H., Zang B., Chen H.
2	TinMan	Yubin Xia, Yutao Liu, Cheng Tan, Mingyang Ma, Haibing Guan, Binyu Zang, Haibo Chen
3	Sentry	Colp p., Zhang J., Gleeson J., Suneja S., Lara E., Raj H., Saroiu S., Wolman A.
4	Armored	Muller T. Spreitzenbarth M.
5	Deadbold	Skillen A., Barrera D., Oorschot P.
6	Droidvault	Li X., Hu H., Bai G., Jia Y., Liang Z., Saxena P.
7	RPMB	Reddy A.K., Paramasivam P., Vemula P.B.
8	CATT	Brasser F., Davi L., Gens D., Liebchen C., Sadeghi A.
9	ARMOR	Ghasempour M., Lujan M., Garside J.

From the operating system point of view, starting with Android 4.0, there are several options, like FDE (Full-Disk Encryption), FBE (File-Based Encryption) and KeyChain.
In [12] there are presented compromise countermeasures for mobile operating systems such as:

- controlled and conditional access to the applications;
- restrictions and user blocking in applications to identify different behaviors;
- monitoring, reporting, and reporting for all user actions in mobile applications;
- achieving accurate procedure for incident response mode;
- updating operating systems on mobile devices;
- encrypt the mobile data;
- using PINs, passwords, and access codes.

Vulnerabilities will always exist, and new ones will be discovered. The goal of mobile application data security is to identify these vulnerabilities to eliminate vulnerabilities discovered and to be prepared for new vulnerabilities.

6 Conclusions

In this paper, we introduced a new approach for identifying the vulnerabilities and exposures that are the most common and represent the highest threat on mobile data. In order to identify those vulnerabilities we started from the list of the generic Common Vulnerabilities and Exposures (CVEs) that are normally used by security experts, and used a search based approach in which we started by a list of common words related to mobile data and based on the retrieved documents, we identified the common vulnerabilities in these documents. After that, we studied the relationship between the extracted vulnerabilities and the different search categories. Accordingly, we proposed a number of countermeasures that the security experts need to consider in order to keep the mobile data secure. The proposed solution CrawVulns can be used for different analyses in future in other fields and for other solutions.

Acknowledgments

Parts of this research have been published in the Proceedings of the 18th International Conference on Informatics in Economy, IE 2019 [14].

This paper was co-financed from the Human Capital Operational Program 2014-2020, project number POCU / 380/6/13/125245 no. 36482 / 23.05.2019 "Excellence in interdisciplinary PhD and post-PhD research, career alternatives through entrepreneurial initiative (EXCIA)", coordinator The Bucharest University of Economic Studies".

References

[1] T. H. Noor, S. Zeadally, A. Alfazi, Q. Z. Sheng, "Mobile cloud computing: Challenges and future research directions" *Journal of Network and Computer Applications*, 115, 2018, pp. 70-85.

[2] A. S. M. E. Yuksel, A. Sertbas, A. H. Zaim, "Implementation of a web-based service for mobile application risk assessment," *Turk J Elec Eng & Comp Sci*, 25, 2017, pp. 976-994.

[3] M. Marian, *Ghid de Securitate Informatică*, Craiova: Universitară Publishing House, 2009.

[4] C. Boja, P. Pocatilu and A. Zamfiroiu, "Data Security in M-Learning messaging services," *International Journal of Computer Communications*, vol. 5, pp. 119-126, 2011.

[5] B. Iancu, T.M. Georgescu, "Saving Large Semantic Data in Cloud: A Survey of the Main DBaaS Solutions," *Informatica Economică*, vol. 22, no. 1/2018, pp. 5-16

[6] M. Gontovnikas, 10 Mobile Security Threats (and What You Can do to Fight Back), 2017, Available at: https://auth0.com/blog/ten-mobile-security-threats-and-what-you-can-do-to-fight-back/

[7] H. Altuwaijri and S. Ghouzali, "Android data storage security: A review," *Journal of King Saud University – Computer and Information Sciences*, In Press, Corrected Proof, Available online: 19 July 2018, DOI: 10.1016/j.jksuci.2018.07.004.

[8] M. Sujithra, G. Padmavathi and S. Narayanan, "Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile data to Cloud" *Procedia Computer Science*, vol. 47, 2015, pp. 480-485.

[9] OWASP mobile security, Available at: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

[10] CVE - Common Vulnerabilities and Exposures (CVE), Available at: https://cve.mitre.org/

[11] Wordcounter, available at: https://wordcounter.com/

[12] M. Raggo, *Mobile Data Loss: Threats and Countermeasures*, Syngress, 16th December 2015, p. 55.

[13] NVD –Vulnerability Metrics, Available at: https://nvd.nist.gov/vuln-metrics/cvss

[14] A. Zamfiroiu, P. Pocatilu, and S. Capisizu, "Mobile Data Vulnerabilities," *Proc. of the 18th International Conference on Informatics in Economy Education*, Research and Business Technologies, Bucharest, Romania, May 2019, pp. 407-412

Alin ZAMFIROIU has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2009. In 2011 he has graduated the Economic Informatics Master program organized by the Bucharest University of Economic Studies and in 2014 he finished his PhD research in Economic Informatics at the Bucharest University of Economic Studies. Currently he works like a Senior Researcher at "National Institute for Research & Development in Informatics, Bucharest". He has published as author and co-author of journal articles and scientific presentations at conferences.

Paul POCATILU graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 1998. He achieved the PhD in Economics in 2003 with thesis on Software Testing Cost Assessment Models. He has published as author and co-author over 45 articles in journals and over 40 articles on national and international conferences. He is author and co-author of 10 books, (Mobile Devices Programming and Software Testing Costs are two of them). He is professor at the Department of Economic Informatics and Cybernetics within the Bucharest University of Economic Studies, Bucharest. He teaches courses, seminars and laboratories on Mobile Devices Programming, Economic Informatics, Computer Programming and Project Management to graduate and postgraduate students. His current research areas are software testing, software quality, project management, and mobile application development.

Sergiu CAPISIZU has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 1997 and National University of Defense in 2005. He holds a PhD diploma in Economic Cybernetics and Statistics, having the title Models and techniques to perform the economic information audit. He is co-author of books and articles in information audit and ICT fields. Also, he has published articles in proceedings of national and international conferences, symposiums, workshops in the fields of data quality, software quality, information audit and juridical aspects in ICT field. He is evaluator of ANEVAR association.