The usage of dependency graphs to test the security of mobile software applications

Antonishyn Mykhailo

Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, antonishin.mihail@gmail.com

Abstract. *Testing the security of mobile software applications by OWASP guidelines was analyzed. Attention is drawn to three levels of requirements in OWASP MASVS and their implementation under the OWASP MSTG guidelines. This guide identifies the processes and methods of testing mobile software applications for vulnerability. This leads to the arbitrary usage of these tools when verifying the feasibility of security requirements for mobile software applications. Overcoming the constraints is suggested by using dependency graphs, given the relationship between the testing stages.*

Keywords: *application security, mobile application security testing, MASVS, MSTG, OWASP, dependency graph.*

I. Introduction and Problem statement

Software applications for the Android operating system are increasing in popularity year by year. Therefore, one of the important aspects of their usage is safety. The security of mobile software applications is analysed by testing for vulnerabilities. For this purpose it is recommended to use the guidelines of OWASP MASVS and OWASP MSTG [1-3].

The requirements for the security of mobile software applications are set out in OWASP MASVS [3]. It defines two levels of requirements (MASVS-L1, MASVS-L2) and sustainability requirements (MASVS-R). The first level sets the general requirements for mobile software applications (MASVS-L1). Whereas the second one deals with the processing of highly sensitive data (MASVS-L2). The MASVS-R level reflects the requirements of preventing the implementation of threats by the user [1, 3, 4]. The feasibility of these requirements is analyzed according to the guidelines of OWASP MSTG [2]. This guide defines the processes and methods of testing mobile software applications for vulnerabilities [1, 2, 4].

However, when testing mobile application security on OWASP guidelines, it is up to the specialist to choose the right steps and tools. This leads, on the one hand, to the arbitrary choice of a sequence of steps and means of verifying the feasibility of security requirements. Whereas, on the other hand, it is difficult to reproduce the obtained results.

II. Problem solution and Results

To overcome these limitations, it is suggested to use dependency graphs [5]. The dependency graph is an oriented graph that displays the ratio of the multiple stages of mobile app security testing according to the selected transitive relationship (for example, the "pre-stage") over it:

$$G = (V, T), \qquad (1)$$

where V – is the set of stages of mobile app security testing according to OWASP guidelines, $V = \{v_i\}$, $i = \overline{1,n}$; T – is a transitive closure R on the set V, $T \subseteq R$; R – is a binary relation on the set V, $R \subset V \times V$.

Then, for example, testing a mobile application server with a static analyzer we get the following usage (1):

v_1 – running on a virtual machine;

v_2 – checking the ability to run on rooted devices;

v_3 – checking the possibility of debugging;

v_4 – checking for obfuscation and protection against tempering;

$$V = \{v_i\},\ i = \overline{1,4},$$
$$R = \{(v_1; v_2), (v_2; v_3), (v_3; v_4)\},\ R \subset V \times V,$$
$$v_1 R v_2 \Rightarrow v_2 R v_3 \Rightarrow v_3 R v_4,$$
$$v_1 T v_4.$$

III. Conclusions

Therefore, the feasibility of mobile application security is tested by OWASP guidelines. The choice of stages, means and sequence of their implementation is the responsibility of the specialist. This makes it difficult to reproduce the results. To prevent this, it is suggested to use dependency graphs in view of the relationship between testing stages.

References

[1] M. Antonishyn, and O. Misnik, "Analysis of testing approaches to Android mobile application vulnerabilities", Selected Papers of the XIX International Scientific and Practical Conference "Information Technologies and Security", Ukraine, vol. 2577, pp. 270-280, November 2019. [Online]. Available: http://ceur-ws.org/Vol-2577/paper22.pdf.

[2] OWASP Mobile security testing guide (MSTG). [Online]. Available: https://github.com/OWASP/owasp-mstg/.

[3] OWASP Mobile application security verification standard (MASVS). [Online]. Available: https://github.com/OWASP/owasp-masvs.

[4] M. Antonishyn, "Android application security assessment," UP2IT conference. [Online]. Available: https://www.slideshare.net/Mykhailo Antonishyn/android-pentesting-189736097.

[5] J. Gross, J. Yellen, and M. Anderson, Graph Theory and Its Applications. Boca Raton, USA: CRC Press, 2019.