Secure Design and Development of Applications in the Cloud and Mobile Ecosystem*

Francisco T. Chimuco[1,2,3][0000−0002−1006−381X], João B. F. Sequeiros[1,2][0000−0001−7206−7771], Tiago M. C. Simões[1,2][0000−0001−8858−0027], Mário M. Freire[1,2][0000−0002−9017−5001], and Pedro R. M. Inácio[1,2][0000−0001−8221−0666]

[1] Universidade da Beira Interior, Covilhã, Portugal
[2] Instituto de Telecomunicações, Covilhã, Portugal
[3] Instituto Superior de Ciências de Educação da Huíla, Lubango, Huíla, Angola

Abstract. We have been witnessing widespread adoption of mobile devices and applications. However, this has not been accompanied by the adoption of good practices in secure development, and there is a considerable gap between software engineering and security engineering. This paper presents a framework, named *Security by Design for Cloud and Mobile Ecosystem* (SecD4CLOUDMOBILE), which was created to assist developers of Cloud-based mobile applications by providing technical guidance, especially for non-security experts, to ensure security and privacy by design. It is a set of tools that allows answering questions commonly asked by software engineers during the process of software development. ChatGPT was integrated into the methods responsible for generating a set of systematized and complete documents, in response to user requests. It is composed of five main modules. The preliminary validation of the tools consisted of the selection of two real use cases, which were applied to the CSRE and CSBPG tools. The results between chatGTP and the platform are similar, which means that there is agreement on the results that should be given to the user.

Keywords: Cloud Computing · Mobile Computing · Security Requirement Elicitation · Security Attack Models · Security Tests Specification and Tools · Security Mechanisms

1 Introduction

Computing paradigms are continuously evolving at a fast pace. Recently, this evolution was mainly due to the emergence and combination of new technologies, namely, Robotics, Cloud Computing [11], Mobile Computing [4,9,15,6],

* The authors wish to thank the Instituto de Telecomunicações. This work was performed under the scope of Project SECURIoTESIGN, with funding from FCT/COMPETE/ FEDER (Projects with reference numbers UIDB/50008/2020 and POCI-01-0145-FEDER-030657) and FCT research and doctoral grants BIM/n32/2018-B00582 and SFRH/BD/1338 38/2017, respectively.

IoT [1,18], Fog Computing [3,2], and Blockchain [12,8,5]. The advancement in communications technologies and the many associated benefits caused the widespread adoption of Cloud-based mobile applications, giving rise to new ecosystems such as Cloud and Mobile [16] and Mobile IoT [6].

The combination of these technologies aims to make up for the shortcomings of one technology over another. This is the case of the Cloud and Mobile ecosystem, allowing to add full communication benefits, storage and computational power to remote and potentially more constrained devices. Unfortunately, such adoption has not always been accompanied by development processes that aim at security-by-design or by-construction, where security and privacy issues are taken into account since inception, and not left to be handled later or ignored.

This paper presents the SecD4CLOUDMOBILE framework. This framework is linked to security engineering, whose purpose is to bridge the gap between software engineering and security engineering.

The remaining part of the paper is structured as follows: Section 2 presents the background of the research. Section 3 presents the proposed framework and the performance evaluation of the framework is addressed in section 4. Finally, the conclusions and future work are presented in section 5.

2 Background

Most of the security issues in the Cloud and Mobile ecosystem have the application layer as their weakest link [13,17]. As this ecosystem is composed by a wide panoply of technologies from very rich subsystems or paradigms such as the Internet, the Cloud, and Mobile, it inherits many the security problems of these technologies [10,7] and faces new threads from the intersections. While there is an attempt to propose solutions to various privacy and security issues for IoT systems [14], these issues remain mostly unresolved for the Cloud and Mobile ecosystem. According to Sequeiros et al. [16], the main challenges are as follows: *a*) *Lack of Specific Modelling and Design Tools for the Cloud and Mobile ecosystem*; *b*) *Heterogeneity of Attack Vectors*; *c*) *Stronger focus on Attack Modelling rather than Threat Modelling*.

As mentioned, there is a large attack surface complexity on a Cloud-based mobile application, which degenerates into most attacks being carried out remotely and exploiting the human factor, with end devices being main targets for attacks. These circumstances clearly motivate the need for security measures that focus on incorporating security-by-construction mechanisms aimed at ensuring the security and data privacy requirements, which is the focus of the research that ended in the development of the proposed framework.

3 The Proposed Framework

Figure 1 contains a high-level architecture of the SecD4CLOUDMOBILE framework, on which five main components are highlighted: (i) the *user interface*, (ii) the *filtering and query processing*, (iii) the *security manager*, (iv) the *storage*

and updates and (v), the *output interface*. The component mentioned in last is additionally responsible for enriching outputs by generating new descriptive text through ChatGPT via the OpenAI API. The *security manager* component allows for the integration of specialized modules that act on the inputs to address a given cybersecurity aspect of secure development (e.g., requirements elicitation).

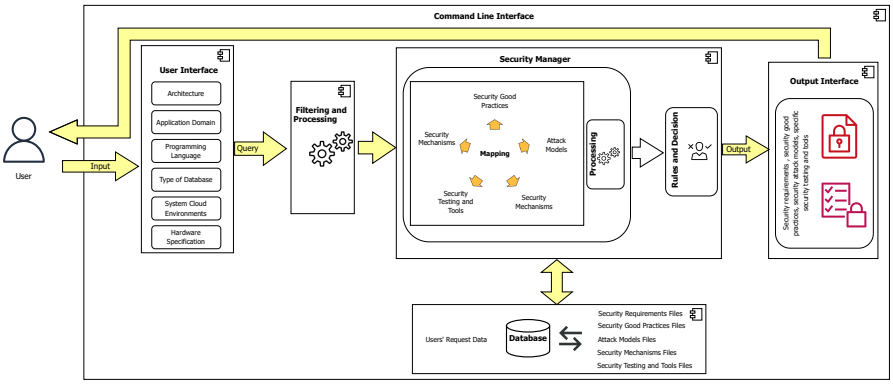

Fig. 1. A high-level architecture of the SecD4CLOUDMOBILE framework.

3.1 Modules Description

At the time of writing, the framework contains five main modules shortly referred to as: CSRE, CSBPG, CMAME, CSME, and C2ST. The CSRE module can be used to request a set of security requirements for a Cloud-based mobile application. The CSBPG module provides users with a set of security best practice guidelines in the application development process. The CSME module generates and provides a set of systematized documentation regarding the security mechanisms that must be incorporated in the coding phase and that must be implemented to ensure the security of the application. The CMAME module generates and provides a set of attack models regarding the threats/attacks that an application may be subject to. Finally, the C2ST module generates and provides a set of recommendations regarding security tests, including the tools to automate them, aiming to ensure that the mechanisms are well incorporated.

3.2 SecD4CLOUDMOBILE Module Implementation

The framework is a multi-platform Command Line Interface (CLI) application and has a set of modules implemented in Python. In addition, the integration of new functionalities, through new modules, is possible due to its modular construction. The complete source code, released under the Apache license, version

2.0 (SPDX-License-Identifier: Apache-2.0), is available from the GitHub of the SECURIoTSIGN project at https://yep.pt/nuOER.

The modules are essentially composed of two main parts: the input collector, which prepares the user inputs and recommendations generated by other modules (which can also serve as inputs), and the output processing, which is responsible for processing the data collected by the input collector. This output processing is responsible for managing each module, such as filtering and processing each response provided by the user, and consequent generation of reports. To enrich the outputs, making them dynamic and more effective (well written), ChatGPT was incorporated via the OpenAI API in the logic part of each of the five modules (in this case, the model used was `text-davinci-003` from `GPT-3.5`).

4 Performance Evaluation

To test the framework, many real test scenarios were described and considered, though only two test scenarios are mentioned herein for the sake of saving space: (i) a smart home scenario, with an automated vacuum cleaner and an integrated security camera, (ii) and a m-Payment system, that allows secure financial transactions through a mobile network. In addition, ChatGPT was also prompted to provide outputs to the same questions, so that we could compare its ability to, e.g., provide recommendations on security-by-design from systems descriptions, in comparison with our tools. When comparing the outputs of the framework with the ones of ChatGPT alone, it was noted that the outputs of the tools are (still) more effective and adequate, but overall they are similar in the type of information, which shows that there is agreement on the results that should be given to the user. E.g., for the two test scenarios considered, the framework recommended 15 and 14 of the (15) expected security and privacy requirements, respectively, while ChatGPT recommended 13 and 11 out of the (15) expected security and privacy requirements, respectively.

5 Conclusions

A extensible framework of tools to aid developers who are actively involved in the design and development of Cloud-based mobile applications was presented herein. It is based on the idea that it is possible to combine and translate answers to an appropriated set of questions and other inputs into security requirements, attack models, recommendations on implementation and security best practices.

The evaluation of the tools is being performed by studying realistic scenarios of the cloud and mobile ecosystem, comparing the results obtained by a human expert, the several tools and ChatGPT. Though the set of tools performs better than ChatGPT at the moment, results also suggest that large language models might be doing security engineering for us in the future. A possible future iteration of this work consists of using the developed tools (and the knowledge that they encapsulate) to fine-tune such models and assess their accuracy.

References

1. Ashton, K., et al.: That 'internet of things' thing. RFID journal **22**(7), 97–114 (2009)
2. Bonomi, F., Milito, R., Natarajan, P., Zhu, J.: Fog computing: A platform for internet of things and analytics. In: Big data and internet of things: A roadmap for smart environments, pp. 169–186. Springer, Cham (2014). https://doi.org/https://doi.org/10.1007/978-3-319-05029-4_7
3. Bonomi, F., et al.: Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. p. 13–16. MCC '12, Association for Computing Machinery, New York, NY, USA (2012). https://doi.org/10.1145/2342509.2342513, https://doi.org/10.1145/2342509.2342513
4. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems **25**(6), 599–616 (2009). https://doi.org/https://doi.org/10.1016/j.future.2008.12.001, https://www.sciencedirect.com/science/article/pii/S0167739X08001957
5. Di Pierro, M.: What is the blockchain? Computing in Science Engineering **19**(5), 92–95 (2017). https://doi.org/10.1109/MCSE.2017.3421554
6. Elazhary, H.: Internet of things (iot), mobile cloud, cloudlet, mobile iot, iot cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. Journal of Network and Computer Applications **128**, 105–140 (2019). https://doi.org/https://doi.org/10.1016/j.jnca.2018.10.021, https://www.sciencedirect.com/science/article/pii/S1084804518303497
7. Gupta, B.B., et al.: Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimedia Tools and Applications **77**, 9203–9208 (2018). https://doi.org/https://doi.org/10.1007/s11042-017-5301-x
8. Gupta, S.S.: Blockchain. IBM Onlone (http://www. IBM. COM) (2017), https://www.isical.ac.in/~debrup/slides/Bitcoin.pdf
9. Imielinski, T., Korth, H.F.: Mobile computing, vol. 353. Springer Science & Business Media (1996), https://books.google.pt/books?hl=pt-PT&lr=&id=AY3RRJnMpXIC&oi=fnd&pg=PR20&dq=Mobile+Computing&ots=Udm7JV0vFG&sig=q6vckxFH3ePX6oK8e_yZA59R7TQ&redir_esc=y#v=onepage&q=Mobile%20Computing&f=false
10. Manadhata, P.K., Wing, J.M.: An attack surface metric. IEEE Transactions on Software Engineering **37**(3), 371–386 (2011). https://doi.org/10.1109/TSE.2010.60
11. Mell, P., Grance, T., et al.: The nist definition of cloud computing (September 2011)
12. Nofer, M., et al.: Blockchain. Business & Information Systems Engineering **59**(3), 183–187 (2017). https://doi.org/0.1007/s12599-017-0467-3
13. Salah, K., Alcaraz Calero, J.M., Zeadally, S., Al-Mulla, S., Alzaabi, M.: Using cloud computing to implement a security overlay network. IEEE Security Privacy **11**(1), 44–53 (2013). https://doi.org/10.1109/MSP.2012.88
14. Samaila, M.G., et al.: Iot-harpseca: A framework and roadmap for secure design and development of devices and applications in the iot space. IEEE Access **8**, 16462–16494 (2020). https://doi.org/10.1109/ACCESS.2020.2965925
15. Senyo, P.K., Effah, J., Addae, E.: Preliminary insight into cloud computing adoption in a developing country. Journal of Enterprise Information Management (2016)

16. Sequeiros, J.B.F., et al.: Attack and system modeling applied to iot, cloud, and mobile ecosystems: Embedding security by design. ACM Comput. Surv. **53**(2) (Mar 2020). https://doi.org/10.1145/3376123, https://doi.org/10.1145/3376123
17. Shirazi, S.N., et al.: The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE Journal on Selected Areas in Communications **35**(11), 2586–2595 (2017). https://doi.org/10.1109/JSAC.2017.2760478
18. Tan, L., Wang, N.: Future internet: The internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). vol. 5, pp. V5–376–V5–380 (2010). https://doi.org/10.1109/ICACTE.2010.5579543