International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Study of Self-Protection in Mobile Applications

Asim A. Al Abri[1], *Nadir K. Salih*[2]

Electrical and Computer Department, College of Engineering, University of Buraimi, Oman[12]

192004@uob.edu.om[1] , nadir@uob.edu.om[2]

ABSTRACT

Business and individuals become more dependent on mobile phones, where the mobility and the fast increment of mobile applications gives an advantage for the rapid growth of the economy and the speed of carrying out the tasks of individuals. The growth of mobile usage is also increasing the risk of attacks and data leakage. Relaying to traditional ways to protect the applications is not enough and it cans trade-off the security against the performance. In this study, we search for a methodology that can provide automated self-protection to protect mobile applications against attacks. This research is based on analysing the protection methods from previous studies and the results they obtained, in order to build a methodology capable to provide self-protection for mobile applications.

Keywords: Applications Attacks, Mobile Applications, Self-Protection, Automated Security.

1.INTRODUCTION

Educating all people about mobile application risks will not be easy and not acceptable for all people. In addition, it needs more time with continuous efforts to achieve the goals. Daily wise, businesses and Individuals are using various mobile applications, which the applications offer office applications, shopping applications, email, and social media applications, and other same desktop functionality. However, these activities can increase also the surface of mobile application attacks, since there are a million web applications that have variabilities that can be exploited by attackers.There are a million mobile applications that have threats and it can exploit user poor knowledge in security, which leads to difficulties to protect the user from all threats depending only on traditional methods. On other hand, many security solutions include automation methods [10], hardware methods [1], coding methods [12], mathematical methods [13], and other methods. Those methods are developed to protect and prevent applications against various security threats. The previous methods are not protecting the user as an asset, where its deals with only the data and applications behaviour. Nowadays security solutions are designed to apply self-protection and self-configuration of the security settings in real-time without human interaction [2]. There are a lot of solutions that have been implemented to introduce approaches for self-protection including (I) Runtime application self-protection (RASP) model and the MAPE-K feedback loop model, (II) Self-protection based on sensors and mini computing devices, (III) self-protection based on coding and software, (IV) self-protection based mathematical algorithms, (V) and Self-protection based on user behaviour monitoring.

2.RELATED WORK

The cyber threats are increased with the increment of mobile applications usage. The security of mobile is insufficient to detect and prevent cyber threats, whereas the current security mechanisms suffer from false positives and false negatives [10]. In addition, the insecure visiting mobile agent where can be compromised by any destination machine [11]. To mitigate those issues, we need autonomic computing and computer security can provide dynamic security configure the security measures in mobile [1]. There are many programming languages such as Java programming can be used to create a self-protection code based on instruction level, where this capability needed for dynamic self-protection methods including integrity process checks and encryption during runtime [12]. RASP and MAPE-K are examples of autonomic self-protection systems. MAPE-K feedback loop includes knowledge, monitoring, analysis, planning, and execution, where the factor of risk should be identified and assessed to activate the self-protection from the loop of MAPE-K [16]. RASP is a model designed to protect applications while running from untrusted user input or abnormal behaviour by comparing application behaviour and the context of that behaviour [5].Table 1 below shows the distribution of research on common topics.

Table 1: Distribution of research on common topics.

Titles	Studies
Self-protection based on MAPE-K and RASP methods	(Yu Y., 2019), [16]
	(Mahmoud , Joshua , & Sam , 2018) [10]
	(Petar&Maraviü , 2016) [14]
	(Danish &Shyam , 2020) [5]
Self-protection using sensors and mini computing hardware	(Aakash , Asad , Abdulrahman , Wilayat , & Maryam , 2019) [1]
	(Eunjoo&Hyeoun-Ae , 2018) [6]
	(SAIDAIAH , M., N., & M. , 2020) [15]
Self-protection based on coding and software.	(Mykola , Sebastien , &Tilo , 2015) [12]
	(Tolga , Lynsay, Natalie , & Colin , 2020) [16]
self-protection based on mathematical algorithms	(Mohamad , Vijey , & Ahmed , 2020) [11]
	(Charilaos&Narges , 2020) [2]
	(Perichappan, 2018) [13]
	(Jingyi& M., 2019) [9]
	(CHIBA & KRICHMAR, 2020) [3]
Self-protection based on user behaviour	(F. & P. , 2018) [7]
	(JianMing , PengWei , Yan , & Shuang , 2016) [8]

3.METHODOLOGY

Different Methodologies has the ability to provide self-protection for mobile applications. Aakash et al, in [1] they introduced framework that provides dynamic security to protect the software and hardware of the mobile device, while Mohammed et al, in [10] they introduced SLAMA approach used for self-protection mobile software by monitoring the process, analyzing the security posture, and providing dynamic security protection. The features of the methodology should be to provide automated protection running in real-time and enhance the security system to be more efficient and intelligent by learning over time. Some Authors introduce taxonomy for how to integrate attack-awareness techniques into mobile applications. It acts as Agent-Driven software component acting autonomously on behalf of its user to design integrated attack awareness. The agent can provide an interface for manual configuration, generating a control of security at runtime in order to provide attack awareness through any mobile application running in the runtime environment. The proposed system must ensure from visiting the mobile agent is not malicious, and prevented from exciting a malicious action. And provide the security principles of authentication, authorization, confidentiality, availability, and integrity.One model used probabilistic to verify the properties of the attacker and system behaviour. The approach is designed and implemented to be capable of self-protection in real-time. Moreover, the approach is fixable enough to be incorporated into the architecture-base system with fewer required changes in the underlying architecture. Other opinions applied the self-monitoring of biological organisms and how to inspire autonomous design. Where the authors created a roadmap that has two sides, the first side about the nervous system, and the second side of the roadmap is describing the possible parallels in engineered autonomous systems.

4.MOTIVATION

Take the advantage of AI deep learning and neurobiology technology. With the growth of mobile technology, there are a lot of wearable devices gathering more raw data related to daily user activities. However, the users are still not used to being supervised. The mobile can collect the raw data of the user's daily activities and user emotions which can be used to build deep learning and behaviour analysis [9].There are many challenges in decision-making applications such as e-commerce, where the user needs to buy one item from a wide variety. The AI agent can help the user by suggesting an item perfectly. These kinds of application providers such as Google and Amazon can provide AI decision-making to help the user. However, still, some exist expect parts of user behaviour prediction and decision-making Support can be improved [13].

The long history of neurobiology is inspiring engineers to simulate neural network systems to create algorithms based on machine learning that can make the systems self-adaptive [3]. For that can give the some motivation identification of researches:

- Find solutions for privacy breaches:

Finding a solution for the poverty of resources, data security, and privacy against unexpected security threats [1]. Losing privacy can negatively affect user confidence in mobile applications. The loss of privacy makes users decide to not install applications when they discovered how sensitive data are leaked by those applications. Because of the aforementioned cases, the system developers are encouraged to build models that can detect malicious apps to make a healthy mobile environment [8].

- The affected performance and the need for improvement

Mobile application performance can be affected by a high false-negative rate or security trade-off against performance in closed-source systems.

The closed-source systems are often remaining the threats undiscovered or discovered but not mitigated due to cost, lack of skills, or trade-off the security against performance [2].

The dynamic analysis approaches suffer from reachability, where the variability is missed because of inputs that fail to reach the variable code. This leads to more false-negative rates. In addition, due to the complexability of Android systems such as granting/revoking permissions, adding/removing apps, and dynamic class loading, the security status keeps changing over time which leads to change the entire security analysis every time, this process will cost the performance of the app and less practical use [10].

- Secure the networks and remote communication:

Networks and remote communication agents are tools that can be used to compromise the systems by exploiting mobile hardware and applications.

Visiting mobile agents can be attacked by a destination machine, and the attack can be executed within the area of the destination machine. The mobile agent is important to perform tasks remotely by home machine.The security reports have highlighted that the security-specific threats to mobile include location tracking and banking transactions. Can occur using built-in hardware such as GPS and Wi-Fi which initializes the installed applications such as location raking or pulse monitoring. To protect the mobile applications, we need adaptive security to secure the built-in hardware of mobile and installed applications based on runtime monitoring. Self-security can adjust the security of the network level of the device [12].

- User behaviour and attack awareness:

The current methodologies and tools need to be changed; otherwise, the security will slow down the development process which leads to insecure applications. To gain improvement in security events, it must integrate attack awareness into the application. Otherwise, the attacks keep developing, and there is the chance to compromise the data without even being noticed [16].

Cybersecurity threats can exploit the user security behaviour, where the user actions are strange and developed over time depending on the change in goals and purposes. User profiling and monitoring user behaviour through user profiling can be used for cybersecurity purposes [7].

5.CONTRIBUTIONSAND EVALUATION

In the mentioned studies, the papers provide four types of contributions which are conceptual or theoretical research, empirical research, and methodological research.The conceptual or theoretical research is used to improve concept or methodology definitions from the original construct.Empirical research used to test a theoretical relation between two constructs has not been tested before. The methodological research it is a type of research used where is a methodologist change on the previous design, the changes lead to reduce the possible problems through measurement methods. A large sample procedure can help to increase the generalizability of the research. Lastly, they enhance the validity of measures through the use of measurement approaches that do not rely on self-reports.The survey research where its meta-analyses work has been done on the search goal. Where the contribution proper for mature researches, where the surveys should exhibit completeness, maturity, depth, and organization.The author evaluates the methodology using two case studies that refer to Insecure Store and ZNN self-adaptive Exemplar to provide news service content to clients.), the authors evaluate the algorithm and heuristics of their application and evaluate the usability. The Algorithm was evaluated using several scenarios includes the decision-making node of the decision-making process from the application.The authors evaluated their application using Emagee tools to measure the efficiency and speed test by record the startup of mobile applications before and after implementation of the approach.The authors evaluated the framework by present the results of qualitative evaluation which focus on accuracy, efficiency, and usability, they present some threats to the validity of the framework by evaluating the computation, memory and energy efficiency. There are research questions about the self-protection of mobile applications such as: have the studies reach maturity.The existing approaches sufficient against the new threats, the best way to reach close to perfection in self-protection techniques. Answering the questions needs effort and more researches to get close answers. Get enough knowledge by answering the mentioned questions leads to useful solutions used to initialize or improve an approach to reach close to perfection in the self-protection of mobile applications.

The table 4.1 below shows the types of contributions and the evaluation methods among the studies.

Table 4.1: Types of contributions and evaluation methods among the studies.

SN	Study	Type of Contribution	Motivation Identification	Evaluation Methods
1	(Aakash, et al,2019)	Conceptual Research	Find solutions for privacy breaches	Use ISO/IEC 91261and ISO/IEC 91262 software quality standards.
2	(Charilaos, et al,2020)	Methodological Research	The affected performance and the need for improvement	Used two case studies that refer to Insecure store & ZNN self-adaptive Exemplar
3	(Danish, et al,2020)	Survey Research	Prevent attacks of common web security attacks	Evaluate the security through recommended 80-90% of common attacks reported by (OWAS Top10)
4	(Eunjoo, et al,2018)	Conceptual Research	Provide integrated application containing instructions, communication, management, measurement the vital signs, and notifications.	The algorithm evaluated the process of the decision-making node in several scenarios. The Heuristics were evaluated by Berini tool. Usability is evaluated by participants interest in the application field.
5	(Farhad et al, 2018)	Survey Research	User behaviour and attack awareness	security requirement evaluation by Report Analysis: which includes Cisco reports, cybersecurity breach reports, and Security Surveys and statistics. The Best Practices Evaluation: includes Cisco Reports, Universities, Kaspersky, National Crime Agency, and National Cyber Security.
6	(JianMing, et al,2016)	Empirical Research	Find solutions for privacy breaches	Measure efficacy and start-up speed using Emagee tool.
7	(Jingyi, et al,2019)	Methodological Research	Take the advantage of AI deep learning.	Evaluation by comparing training time and production using a large public dataset.
8	(Mahmoud, et al,2018)	Empirical Research	The affected performance and the need for improvement	The evaluation is based on three statements: a) efficient is an approach compared to the complete analysis approach, b) effectiveness of the approach to minimize unnecessary disruption of security policies enforcement, c) effective of approach in detecting and preventing security attacks in applications.
9	(Mohamad, et al,2020)	Methodological Research	Provide protection to mobile agents against the destination machine when acting as an attacker.	Evaluation based on metrics compared with other works where it counts the points of each work depends on security requirements such as confidentiality, integrity, availability, anonymity, ..etc
10	(Mykola, et al,2015)	Methodological Research	Secure the networks and remote communication	Evaluate the framework by presenting the results of qualitative evaluation which focus on accuracy, efficiency, and usability.

6.DISCUSSION

The main topic of this research is “Self-protection for mobile application”, in this research we looking for a methodology that can provide protection for mobile users autonomously without the need for human interaction. There are a lot of classifications that have been implemented to introduce approaches for self-protection including (I) Runtime application self-protection (RASP) model and the MAPE-K feedback loop model, (II) Self-protection based on sensors and mini computing devices, (III) self-protection based on coding and software, (IV) self-protection based mathematical algorithms, (V) Self-protection based on user behaviour.Our problem statement is to mitigate vulnerabilities and provide self-protection for mobile applications from various attacks using an automated self-learning system that has the ability to protect the mobile application. And based on what was mentioned, we need a methodology that provides a self-protection adoptive dynamically can protect the mobile application from attacks, and enhance the security mechanism to be more efficient by learning over time.

7.CONCLUSION

Security and performance do not flow in the same direction, the high performance in applications means sacrificing protection. Here comes the need for automated self-protection to enhance mobile application security. In the next phase of this research is to build a methodology that has the features of automation, self-protection, and self-learning in order to protect the applications from attacks and data leakage.

References

[1]Aakash , A., Asad , M. W., Abdulrahman , A., Wilayat , K., & Maryam , S. (2019). Adaptive Security for Self-Protection of Mobile Computing Devices. Mobile Networks and Applications.

[2] Charilaos , S., & Narges , K. (2020). Design and Implementation of Self-Protecting systems: A Formal Approach. Future Generation Computer Systems, 421– 437.

[3] CHIBA, A. A., & KRICHMAR, L. J. (2020). Neurobiologically Inspired Self-Monitoring Systems. 1 - 11.

[4] Dakic, M. (2021). BEST WAYS TO TRACK USER BEHAVIOR IN MOBILE APP. Retrieved from zesium: http://zesium.com/best-ways-to-track-user-behavior-in-mobile-app/

[5] Danish, M., & Shyam , G. (2020). A Survey on Web Application Security. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 223-228.

[6] Eunjoo , J., & Hyeoun-Ae , P. (2018). Development of the IMB Model and an Evidence-Based Diabetes Self-management Mobile Application. Healthc Inform Res.

[7] F. , F., & P. , L. (2018). Observation Measures to Profile User Security Behaviour. International Conference on Cyber Security and Protection of Digital Services (Cyber Security), (pp. 1-6). Glasgow.

[8] JianMing , F., PengWei , L., Yan , L., & Shuang , D. (2016). Android App Malicious Behavior Detection Based on User Intention. IEEE TrustCom/BigDataSE/ISPA, (pp. 560-567).

[9] Jingyi , S., & M., O. (2019). Learning Mobile Application Usage - a Deep Learning Approach. 18th IEEE International Conference on Machine Learning and Applications (ICMLA), (pp. 287-292).

[10] Mahmoud , H., Joshua , G., & Sam , M. (2018). Self-Protection of Android Systems from Inter-component Communication Attacks. 2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 726-737.

[11] Mohamad , A. S., Vijey , T., & Ahmed , A. (2020). Achieving self-protection and self-communication features for security of agent-based systems. International Research Journal of Engineering and Technology (IRJET), 1 - 9.

[12] Mykola , P., Sebastien , K., & Tilo , M. (2015). Dynamic Self-Protection and Tamperproofing for Android Apps using Native Code. 10th International Conference on Availability, Reliability and Security, (pp. 129-138). Germany.

[13] Perichappan, K. (2018). Greedy Algorithm Based Deep Learning Strategy for User Behavior Prediction and Decision Making Support. Journal of Computer and Communications, 45-53.

[14] Petar , ý., & Maraviü , ý. (2016). The Framework of Runtime Application Self-Protection Technology. 17th IEEE International Symposium on Computational Intelligence and Informatics, (pp. 81-86). Budapest, Hungary.

[15] SAIDAIAH , B., M., C. S., N., M. N., & M. , K. V. (2020). GPS Based Self Protection System for Women. ICONIC RESEARCH AND ENGINEERING JOURNALS, 220-224.

[16] Tolga , U., Lynsay, A., Natalie , C., & Colin , M. (2020, 8 15). A Taxonomy of Approaches for Integrating Attack Awareness in Applications.

[17] Yu Y., N. Y. (2019). Assessing Security and Privacy Behavioural Risks for Self-Protection Systems. Engineering Adaptive Software Systems, pp. 135-147.

[18] Paolo , A., Elvinia , R., & Patrizia , S. (2015). Modeling and Analyzing MAPE-K Feedback Loops for Self-adaptation. 2015 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, 13 - 23.

[19] Nadir K Salih, Tianyi Zang. Variable service process for SaaS Application.Research Journal of Applied Sciences, Engineering and Technology. vol. 4, Issue 22, 2012, pp 4787-4790 EI.

[20] Nadir K Salih, Tianyi Zang, Mingrui Sun. Multi-database in healthcare network. International Journal of Computer Science Issues, vol.

8, Issue6, No3, 2011, pp 210-214. EI (20123715432268).

[21] Nadir K Salih, Tianyi Zang, G.K. Viju, A Mohamed. Autonomic management for multi-agent system.IJCSI, vol. 8, Issue 5, No 1, pp 338-341, 2011.EI (20123415362715).

[22] Nadir K Salih, Tianyi Zang. Need of Autonomic Management SaaS Application. International Journal of Computer Science Issues , 2016.

[23] Nadir K Salih, Tianyi Zang. Survey and comparison for Open and closed sources in cloud Computing. International Journal of Computer Science Issues, vol. 9, Issue 3, No1, 2012, pp 118-123. EI (20122815240979).

[24] Eman.M-Fageer, Nadir K.Salih. Self-configuring Booking SaaS Application.Red Sea University Journal of Basic and Applied Science.Vol.2 Special Issue (3), 2017.

[25] Amin, Fatima M H, Nadir K.Salih. New Model to Achieve Software Quality Assurance in E-Learning Application. International Journal of Computer Science Issues (IJCSI); Mahebourg 14.3 (May 2017): 65-69.

[26] Eshtiag A Abd Elrhman, Nadir K Salih. Modeling Variation in SaaS Application.International Journal of Computer Science Issues (IJCSI).Volume15 Issue3Pages22-30.2018.

[26]Salih NK,H.Elbashier , Zang T,Eshtiag A Abd Elrhman. Self-Diagnosis of Diabetes Using CBR Algorithm.Journal of Computer Science & Systems Biology. Volume11 Issue3 Pages 235-239.2018

[27] Amin, Fatima M H, Nadir K.Salih. Implementing the System, Instructor and Student Model to Achieve Required Software Quality Assurance. Research Journal of Applied Sciences, Engineering and Technology; pp 30-42,2019.

[28] Nadir K. Salih, Abdel-hafiz A. Khoudour, Mawahib S. Adam, Samar M. Hassen "Autonomic Computing Architecture by Self-defined URI" International Journal of Computer Trends and Technology 68.3 (2020):1-6.2020

[29] Nadir K.Salih , Hanan Ahmed , Nada A. Mohamed Nour , Eshtiag A. Abd Elrhman. Optimization of QoS Requirements For Applications. International Journal of Computer Engineering and Technology (IJCET).Volume12, Issue2, p:1-10,2021.

[30] Nadir Kamal Salih, Self-Diagnosis of Cancer Using Case Base Reasoning Algorithm. International Journal of Research in Engineering, Science and Management. Volume4, Issue6,P: 24-28,2021.

[31] Amal S. Al Maamari ,Nadir K. Salih. Study of attacks on wireless Network.International Journal of Computer Engineering and Technology. Volume 13, Issue 2, May – August 2022, pp. 21-26

[32] Nadir K.Salih1,Hanan Ahmed. Survey on QoS for Applications.International Journal of Research Publication and Reviews.Vol 3, no 6, pp 2157-2164**,** June 2022