A FRAMEWORK FOR ADAPTIVE SECURITY SYSTEM

Ahmed Alaa Al Hamami
Computer Science department. Amman Arab University
Amman, Jordan
Iraqiboy23@gmail.com

Akram M. Othman
Computer Science department. Amman Arab University
Amman, Jordan
Akram.othman@gmail.com

Abstract-**During the lifecycle of any software system, several situations faced and none of them defined at the design time. That means there is a need to be able to place on the software the adaptation to the environment and to the demands. This paper demonstrated two frameworks (Architectural approach for self-managing security service and Contexts sensitive Adaptive Authentication) for the adaptive security and compare them to recognize the advantages and drawbacks for each of them. The aim of this research is to propose a hybrid framework for new adaptive security method that contains the advantages of the two frameworks and avoids their drawbacks. This research compares the three adaptive security frameworks (Architectural approach for self-managing security service, Contexts sensitive and the proposed approach which is named as Hybrid approach) to check the performance. It has been found that the proposed hybrid framework is executed very fast due to its implementation of the adaptive security approach in a simple way and in a short time.**

Keywords- **Security; framework; Adaptive; Hybrid approach; performance.**

I. INTRODUCTION

For the purpose of the secure future applications, various security features must be considered. There are many reasons that security topic becomes a hot subject [Al-Hamami and Alsaadoon, 2015]. The traditional security system contains a predefined procedure to stop the violations. This procedure applied according to conditions and threat features. If these conditions not met, the procedure fails. Most of the researchers and developers [Al-Hamami AH and Al-Khashab RA, 2014] try to use flexible procedures that do not depend completely on predefine conditions such as Data Mining (DM) [Al-Hamami AH and Alawneh TN, 2010], Artificial Immune System (AIS) [Suha et al, 2013], Intrusion Prevention System (IPS) [Al-Hamami AH et al, 2006]……. etc. The new approach of the security system should be flexible and compromise the new security requirements. Its action not predefined to fixed conditions but changes according to the variation of the security requirements; this is what we call Adaptive Security (AS) [Elkhodary & Whittle, 2007].

Therefore, this research applied two frameworks of security adaption that have different framework and then propose a hybrid framework to get a better results. By comparing the three approaches, we can recognize the best one.

II. METHODOLOGY

The proposed framework compares between two approaches (self-managing security service and Contexts sensitive), then collects the advantages and avoid the drawbacks. The proposed hybrid framework is created from the advantages of the two frameworks and by avoiding their drawbacks. Then, the three frameworks will be compared in their performance to recognize the best performance. The test was carried out into two different environments, error and correct testing.

III. THE PROPOSED FRAMEWORK

The proposed model attempts to use traceability as a means to understanding the relationship between security requirements and security policies through implementing two types of adaptive security approaches based on **(Evesti, A., and Ovaska, E., 2013).** These approaches are Context sensitive adaptive authentication and Self-Managing security services. Then the proposed model presented a framework by mixing the two approaches to achieve an appropriate security adaptation.

The proposed framework focused on the user data stored and processed when the context is unknown or when the usage context of application changes. In this case, the model proposed an approach to determine the context of whether it is reliable or not. The determination done through the implementation of the first framework and the second one. Then combine the two frameworks and show which is best for the user between the three frameworks to minimize the risk of threats and to maintain the security requirements despite changes in the usage context.

In this paper, SQL server 2010 database is used to check the performance of the frameworks. Thus, it has been used the database to run several experiments and to check the outcomes of the frameworks from these experiments. Therefore, the researcher decided to choose and retrieve the 830 records in database that have data types (Integer & string) and data sizes (313 kilo bytes).

The following is the description of the two chosen frameworks. The advantages and the drawbacks of each framework have been explained.

A. "An Architectural Approach for Self-Managing Security Services". In **[Russello and Dulay, 2009],** authors discussed the means policies of ESCA (Event, State, Condition, and Action). The process of the Self-Managing Security Services Architectural Approach is one of the most important points for the system process in a safe manner, which is the first step in entering any system.

Therefore, this method depends on IP address & MAC address for the input devices. It will represent an accredited password that used for each user in the system because it is very difficult to repeat this MAC to another device and this distinguishes it from other methods. However, the disadvantage of this method requires time to carry out the verification process and this will observed through the results. Self-managing systems for adapting the security focused on for providing security as a one-size-fits-all solution results in a system that is far too rigid to accommodate the needs of various application spaces.

B. Context Sensitive Adaptive Authentication Method [Hulsebosch et al, 2007], the context information used to augment or replace the traditional security measuring by making them more adaptable to a given context and thereby work to less meddling. It exploit by combining location information obtained from different sources which are related and available to the user. The trust in the identification of the user can be expanded impressively. The level of trust in the identity of the user is combined to the probability that the user is at a specific location. This

probability is used as a measure to parameterize the authentication level of the user making it in thereby considerably more versatile to changing situational conditions. In the Context Sensitive Adaptive Authentication the user is not restricted in writing the characters in large or small size because the system will depend on understanding all the input and connecting between of them in a method to achieve authenticates and match the accredited original password for this user.

C. Hybrid Framework (the proposed method), this research proposed a hybrid framework for security authentication which contains the advantages of the two types of the concerned frameworks and these are: an Adaptive Context Sensitive Adaptive Authentication Method and Approach for Self-Managing Security Services.

Due to the speed of the first type in the Context Sensitive Adaptive Authentication adopted in the choice of password, but the accuracy may be weak and this observed in the results obtained from experiments. The second type is the Architectural Approach for Self-Managing Security Services when it depends on the IP address & MAC address, but it takes longer to perform the verification process.

Therefore, the speed of knowing the password will based on the methodology used in determining it. Then, followed by specifying the accuracy of the user's identification through the IP address & MAC address. Which led to building a hybrid model that enables the user to use the user's knowledge accurately and quickly.

The functionality of the proposed framework is explain in Algorithm (1).

Algorithm (1):

Input: Info

Output: Estimated Time

Step1: Start Algorithm

Step 2: The user registered the begging of start time

Step 3: The user determine the server name for retrieved database

Step 4: The user registered user-name & password

Step 5: The user set specific code

Step 6: Set (x) as length of specific code

Step 7: For i=0 to x

- Y=specific code [i]
- Z= set status of (y) is symbols, character (upper case or lower case) or number.
- Searching (z) in database
- If (z) is founding in database then
- I=i+1
- Else go to step 10

Step 8: Retrieved database based on specific code

Step 9: Registered end time

Step 10: Calculate estimated time based on begging time and end time

Step 11: End Algorithm

TABLE (1) shows the comparison of the three frameworks.

TABLE (1) Advantages and disadvantages of the concerned algorithms

Algorithm name	Advantages	Disadvantages
Self-Managing Security Services	It is very difficult to repeat MAC address on another device.	It requires time to carry out the verification process due to its dependent on IP address and MAC address
Context Sensitive Adaptive Authentication	Saving user's times when they change characters between the lower and upper case.	Possibility of fake user to reach the correct password because of the matching probability of random password.
The Proposed Hybrid Algorithm	It is fast by using speed of "Context -------"in the choice of password. Accuracy is very good because it use the performance of verification process in "Architectural ---". It is easy to upgrade the algorithm by adding more features to it.	We avoided the disadvantages of the concerned two algorithms.

IV. TESTING RESULTS

The researcher builds a model to utilize two types of the adaptive security system. This approach is evaluation primitives including Context sensitive adaptive authentication, Self-Managing security services, and the proposed hybrid frameworks. The three frameworks have tested in two procedures, the first one is the correct implementation of each case and the difference between them based on the time and the second procedure is the testing of error status in each case. Figure (1) shows the Block diagram of the Test Model.

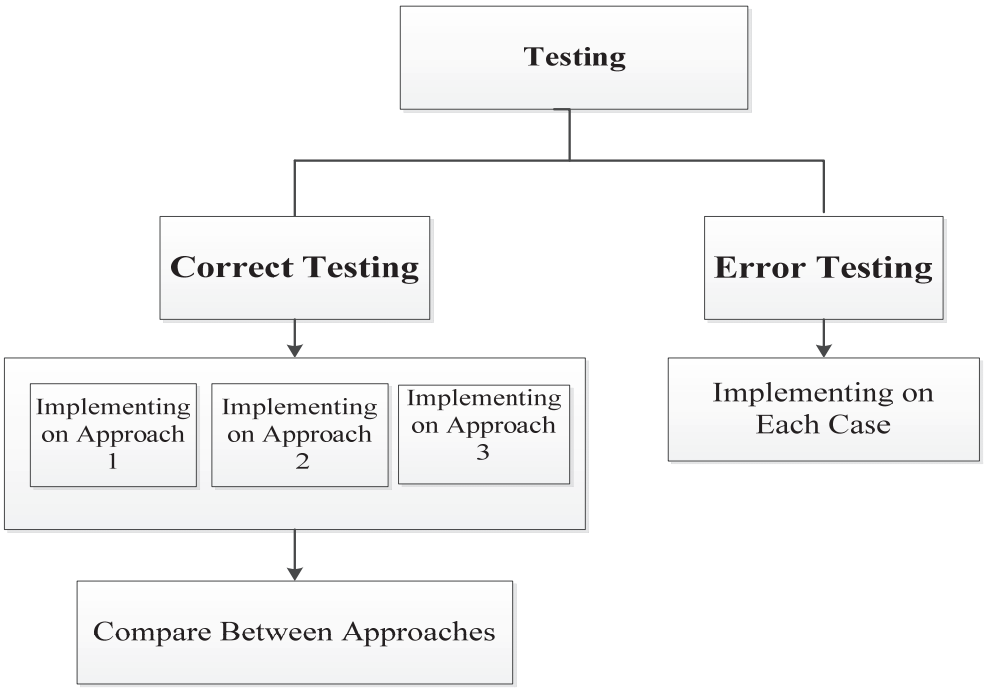

Figure (1) Block diagram of Test model

A. Correct Testing producer

The first procedure has implemented all the correct situations for each approach. The experiment results been obtained through the implementation of each method as in TABLE (2). The experiment has been done by using two different databases and different computer architectures. The Tables show the estimated time of each model compared with the proposed framework. TABLES (2 & 3) show the Experiment Results using Computer 1 and the two databases.

TABLE (2): Experiments Results using Computer 1 and the two databases.

Experiment Number	Experiment Name	Estimated Time of Experiment (per milliseconds)	Data Base Number
1	Windows Authentication of Self-Managing	3.34	DataBase#1
		5.22	DataBase#2
2	Password Authentication of Self-Managing	16.68	DataBase#1
		18.56	DataBase#2
3	Contexts Sensitive Authentication	2.79	DataBase#1
		4.67	DataBase#2
4	Proposed Approach	0.03	DataBase#1
		0.05	DataBase#2

TABLE (3): Experiments Results using Computer 2 and the two databases.

Experiment Number	Experiment Name	Estimated Time of Experiment (per milliseconds)	Data Base Number
1	Windows Authentication of Self-Managing	2.32	DataBase#1
		4.63	DataBase#2
2	Password Authentication of Self-Managing	14.75	DataBase#1
		17.06	DataBase#2
3	Contexts Sensitive Authentication	1.77	DataBase#1
		3.12	DataBase#2
4	Proposed Approach	0.02	DataBase#1
		0.04	DataBase#2

From Tables (2 & 3) we can see that the result of the proposed framework is excellent when we compare it with the results of the Windows Authentication of self-Managing and Contexts Sensitive Authentication. This represented in the hybrid approach that considers the best time for experimental depends on a speed for Authentication of Self-Managing with accuracy from Context Sensitive of Authentication.

B. Error Testing producer

This section is use to find the relative error of the testing is each case of approaches to determine if a user is trying to break into the system or is just making common mistakes. It declared the results, which were obtained through the implementation of the program, which is, listed the following:

- If the username is not register in the authentication list of Self-Managing Security Service approach, the system denied the user from enter to the system because the comparison is implemented based on MAC address and username.
- If the password is not registered in the authentication list of Self-Managing Security Service approach, the system denied the user from enter to the system because the comparison is implemented based on MAC address and password.
- If the username or password is incorrect of Self-Managing Security Service approach, the system denied the user from enter to the system because the comparison is implemented based on MAC address and (username or password).
- If the verification code is incorrect in the Contexts Sensitive Adaptive Authentication approach, the system will display the notification to the user.
- If the password as verification code is incorrect in the Hybrid approach, the system will display the notification to the user.

V. CONCLUSIONS

This paper developed a framework to compromise security adaptation approaches. The framework constitutes of three viewpoints, namely, adaptation, security, and lifecycle viewpoints. The adaptation viewpoint concentrates on the used adaptation model. The security viewpoint covers software security related properties.

Adaptive security is an approach to safeguarding systems and data by recognizing threat related behaviors rather than the files and code used by threats definitions. The essence of the approach is the ability to adapt and respond to a complex and constantly changing environment.

We studied two approaches Architectural approach for self-managing security service and Contexts sensitive is adaptive authentications to recognize the advantages and drawbacks of each of them. From these features, we design a framework we call it Hybrid framework. Then we compare the execution time for the three frameworks and we find that the hybrid framework is much better than other two.

REFERENCES

[1] Al-Hamami A H, Al Hamami M A, and Hashim S H. (2006). Applying Data Mining Techniques in Intrusion Detection System on Web and Analysis of Web Usage. *Information Technology Journal* 5(1): pp.57-63,. Asian Networks for Scientific Information.

[2] Al-Hamami A., and Alawneh T N. (2010). "Developing a Host Intrusion Prevention System By Using Data Mining", Thesis of Master in Computer Science, Graduate College of Computing Studies, Amman Arab University for Graduate Studies,.

[3] Al-Hamami A H and Al-Khashab R A. (2014). "Cloud Authentication method Based on Multiple Passwords Technique", Journal of Advanced Computer Science and Technology Research, Vol. 4, No. 2, June 2014, 33-39.

[4] Al-Hamami A H and Al-Saadoon G M W. (2015). "Security concepts, Developments, and Future Trends", Chapter one, Handbook of research on Threat Detection and Countermeasures in Network Security, Advances in Information Security, IGI Global, USA.

[5] Elkhodary. A and Whittle, (2007). "A Survey of Approaches to Adaptive Application Security" in Proceeding of the software Engineering for adaptive and Self-Managing systems Workshop, pp. 16-23 , Minneapolis, Minn , USA, MAY.

[6] Evesti. A and Ovaska. E, (2013). "Comparison of Adaptive Information Security Approaches", ISRN Artificial Intelligence, Volume 2013, Article ID 482949, 18 Pages.

[7] Hulsebosch, R. Bargh, M. Lenzini, G. Ebben, P. And Iacob, S. (2007). "Context sensitive adaptive authentication" in Smart Sensing and Context, G. Kortuem, J. Finney, R. Lea, and V. Sundramoorthy, Eds., pp. 93–109, Springer, Berlin, Germany.

[8] Russello, G and Dulay, N, (2009). "An architectural approach for self-managing security services" in Proceedings of the IEEE International Conference on Advanced Information Networking and Applications Workshops, pp. 153–158, Bradford, UK.

[9] Suha A, Abu Zitar, and Al-Hamami A H, (2013). "Virus Detection using Clonal Selection algorithm with genetic Algorithm (VDC Algorithm)," Applied Soft Computing, ELSEVIER, 13, 239-246.