Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, No. 2, March : 2024

EVALUATING LAYERED MODEL FOR AUTHENTICATION

Shailesh Kumar Sharma, Scholar, Dr. C. V. Raman University Bilaspur
Dr. Laxmikant Tiwari, Assistant Professor, Deptt of Computer Science, Dr. C. V. Raman University Bilaspur

Abstract
In today's era one of the most prevailing security threat is identity theft. Authentication is an imminent process that tries to resolve the problem by verifying an individual's identity, who wants to access the resources of a system. In view of overwhelming ever-growing use of different authentication scheme their associated cost cannot be ignored. Consequently, it is identified as a requirement for authentication - though it is not a part of the general threat model till now. Moreover, there have been many efforts to estimate the usability of authentication system. However, in particular Efficiency aspect has not been calculated. This paper focuses on importance of Efficiency in password authentication. The efficiency model tries to explain the principles and indicators considered while designing a system for their efficiency. A layered model of Efficiency helps in understanding the different aids required for an efficient authentication system.
Keywords— efficiency, authentication, usability, password, effort

INTRODUCTION

Efficiency in the layman terms can be sought as the potential to construct or do something without deteriorating time, energy or material. It makes use of all the inputs while obtaining the great amount of outputs. "Efficiency relates to the use of all inputs in producing any given output, including personal time and energy." [1].The precise focus on "efficiency" might suggest that the specific meaning of the notion is always clear. Rather an author stated [2] that the "most efficient" algorithm should be the fastest and concluded that the time is an important factor for considering the efficiency of an algorithm. Table I shows that maximum number of authentication schemes whether it is machine centric schemes or user centric schemes have not considered Efficiency more than speed and time computation. However, in computer science different types of efficiency can be distinguished such as algorithmic efficiency and storage efficiency, each with their own definite meanings. All of these efficiencies may cite to increase the output by utilizing minimum amount of inputs. However, the extent of maximization may depend on input and output variables. Likewise, the efficiency may differ having the same inputs and outputs but different working scenarios.

Password Based Authentication (PAS) is a type of Knowledge based authentication in which knowledgeable information such as passwords is kept as a secret from any other individual for access to a system [3]. Despite of the security problems, password authentication has a major influence on the internet for the last five decades. As the cost per user is negligible, passwords help the new start-ups such as Facebook or Linkedin a fair chance to grow themselves [4].

A simple browser can help us to access any financial account or a social networking account protecting the diversity of requirements. However, easy guessable passwords are chosen by users [5] and reused among various accounts [6]. Hence, users were found out to be the weakest link in the chain. It has been seen that the hackers study more about the user's behavior and psychology than security designers. Adams and Sasse [7] also revealed that security designers need to communicate more with the human link to understand their psychology to come up with a user centered design. Initially a user had only one account for which only one password was required. But within a decade, the amount of users has increased enormously making it to almost 10 passwords [8]. Guillaume predicted that by 2020, users will have more than 200 online accounts. So, take restorative action towards the problem efficient password authentication measures should be evolved.

While authentication system on a whole can produce efficient results, this does not necessary imply that every stakeholder such as user, information security expert or developers are also valuing the

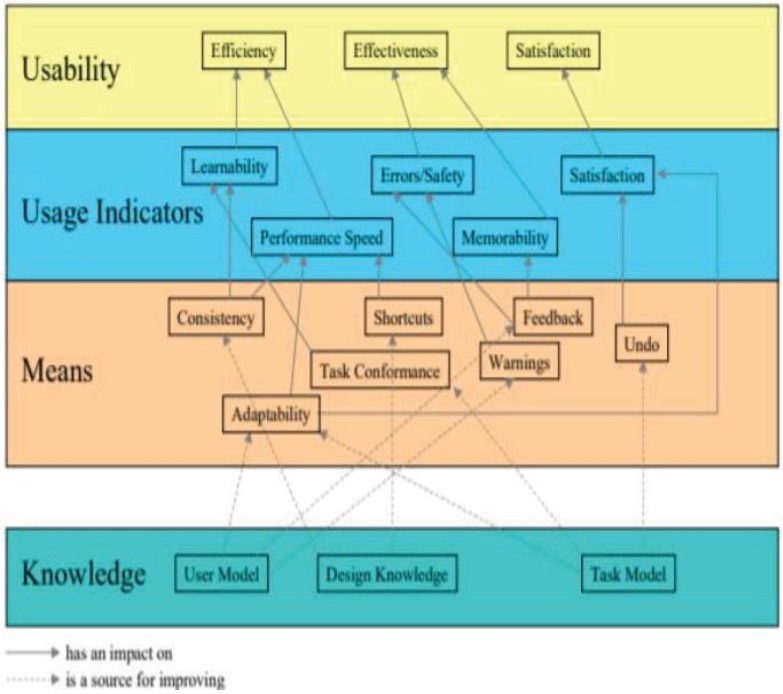
results so produced. This calls for other dimension of efficiency which could address the problem whether the authentication is done with right amount of resources.

So, further sections of the paper will review the elaborative definition of efficiency considering both user and the machine. Thereafter, we start with explanation of efficiency model which comprises of goals, primary and secondary attributes and their knowledge domain.

BACKGROUND

Researchers have defined efficiency in usability models as user efficiency, workflows, productivity, time efficiency, economic efficiency as well as resource efficiency. Van et al., [30] has broken down usability into efficiency, effectiveness and satisfaction and described a layered model for approaching the directed terms. Figure 1 shows the usability layered model. In this paper, we also took inspiration from the model and tried to segregate efficiency from usability and derive a layered for it. Many Experts have proposed several definitions for Efficiency as follows:

- Nielson [9] described the User Efficiency as the time user needs the computer to complete their tasks. He described User Efficiency as different from computer response time as faster response time always doesn't means that users can complete their task efficiently.
- Quesenbery [10], [11], [12] explains that navigation workflows and design elements, such as shortcuts, buttons have a great effect on Efficiency. He suggested that efficiency depends on the context of use and requirements. For example, a manger will see efficiency as a "time on task" problem whereas a worker will see as a problem of error tolerance and support.
- Alonso-Ríos [13] described efficiency into four sub attributes constituting of Efficiency in Human Effort, Efficiency in task execution time, efficiency in tied up resources and efficiency in economic cost.
- MUSIC [1] - is defined as the "Effectiveness related to the cost of performance"
- Gupta et al [14] proposed an efficiency taxonomy in which he divided the attributes of efficiency as Resource, Time, Economic Cost, Documentation and User Effort.



It has also been seen that no password authentication scheme has computed the efficiency factors relating both user centric scheme as well as machine centric scheme. Hence, defining Efficiency as a whole attribute to be considered while designing a password authentication system.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, No. 2, March : 2024

TABLE I. PAS CONSIDERING EFFICIENCY

Password Authentication	Year	Techniques		Efficiency
		Machine Centric	User Centric	
Morris & Thompson[15]	1979	P		
Shamir [16]	1985	P		
Jobsuch & Oldehoeft[3]	1989	P	P	
Adams & Sasse[7]	1999		P	
Kumar[17]	2004	P		P
Renaud[18]	2004		P	P
Bonneau et al[5]	2012		P	P
Katz et al[19]	2011	P		P
Qian et al[20]	2012	P		P

EFFICIENCY –A LAYERED MODEL

The efficiency model tries to explain the principle indicators considered while designing a system for their efficiency, Figure II shows a layered model of Efficiency that help in understanding the different aids required for an efficient authentication system. The highest level defines the goals needed to fulfill while designing an efficient password system. To achieve the desired goals, we start from the basic level of knowledge domains and find out our primary and secondary indicators to reach our desired goals. Following is the detail description of the layered model: -

Goals

Efficiency is one of the major requirements of any authentication mechanism. Authentication Efficiency can be broadly considered in two forms [21]. First, the mechanism should be efficient, it should minimize overhead incurred in the authentication process and the usage of resources - processing time, storage, communication etc. Secondly, mechanism should do considerable value addition by reducing the cost indicative of good security performance, utility etc. Hence the two major goals for considering Efficiency in Password authentication will be considered as follows: -

- Minimize Overheads of resources
- Value addition by reducing cost indicative of utility, good security performance etc.

Depending upon the critical scenario, the overhead of strong authentication may be tolerated. Otherwise, simple-tocomplex graded multi-factor authentication may be prescribed. However, in all cases effectiveness must be an essential and reduced overhead with increase efficiency would be certainly desirable in ever growing pass-wordinevitable systems. Efficiency is more important than anything in both the two forms when considering the authentication mechanism in communication protocol.

Knowledge Domains

If we propose to design any efficient mechanism, we have to look towards the mechanism from the usability view point. Usability as quoted by [30] is the “good” design viewpoint of Human Computer Interaction. Usability can be improved from the evaluation by the user and from the available knowledge gathered during designing. The available domain of knowledge is the primary source of data. The knowledge domains for designing password based authentication can primarily be Humans, Machine Design and Task [31]. The knowledge domains are described briefly as follows: -

- Human Domain/User Model: Users are the most important part of the knowledge domain as the system designed is to be used by them. However, problems related to them still feel ignored [7]. Information processing tasks such as searching, scanning and decision making are few of the hurdles humans goes through [32]. It has been observed that there is a mismatch between the actual abilities of the user and required abilities that is expected by the system [31]. Evaluation from the user can be gathered by questionnaire, interviews and many more. Hence, the user model describes how the user

can interact with the password design and how the changes in context or data attribute changes their behaviour.

- Machine Design Domain/Machine Design Model: The person who designs or develop password authentication mechanisms obtain skills and expertise during their projects and applies that knowledge in the latter projects. The knowledge can be retrieved from the literature as well as the experiences incurred during the project. The design gives guidance about the overall project to the team. Hence, the knowledge gained during machine design phase can be useful during the design of passwords and protocols.
- Task Domain- Task Analysis is a technique that determines the behavior of elements while performing a task [33]. The task domain knowledge helps us to disclose the level of expectations; authentication method poses on users [34]. Hence, what type of attributes the task is requiring at that time or what is the context of use can be gained from the task model.

Efficiency Sub Attributes

In order to achieve the efficiency goals, the efficiency attribute has been further classified into sub attribute [14]. In HCI or usability terms efficiency can be computed by the usage of resources in relation to the achievement of the objective of the user. Therefore, Efficiency for Authentication is reflected in the following four sub attributes.

- Efficiency in User effort – It refers to the level of effectiveness achieved to the mental and physical effort needed to authenticate users.
- Efficiency in Time – It refers to the level of Effectiveness achieved to the time needed to authenticate users and system to respond.
- Finance- It refers to the level of effectiveness achieved to the total cost of the system including the system and the consumables.
- Resources- It refers to the level of effectiveness achieved to the total resources used including both human and material.

Efficiency Primary Indicators

The efficiency primary indicators are the factors which are directly affecting the efficiency of a password authentication system. These are the indicators of efficiency which can be observed when users are at work. Following are the factors which are responsible on the first level: -

- Incursion- Users disabilities can be in the form of cognitive, mobility or sensory. Every mechanism excludes at least one type of disability; hence a little shortfall is assigned to that mechanism. [18]. so, to incorporate all types of users, the user effort has to be considered.
- Special Requirements- The least level of system requirements need to support the authentication mechanism (hardware, software or both) is addressed here [18]. Hence, it caters to the least physical effort required using least equipment cost.
- Learnability- Learn-ability refers to the time duration a user takes to learn some actions. Efficiency increases as the ability to learn increases. [22] Password guidance can be referred as the depiction of support given to the users for selecting a password such as minimum selection tips etc. [23].
- Memorability- Precise recall of the secrets is followed for logging in a password authenticating system; hence the slightest mistake will make your system access fail. A user writes down a password that is hard to recall, ensuring that it is not forgotten but undermining its confidentiality [24]. But, if the password is compromised it will be a greater setback [7], [25]. Hence, the password composition policies should be so chosen that it makes a trade-off between memorability and security.
- Password Storage space – It refers to the Space required to store password information in a file, in a non-file, or in another system for authentication [3]. In limited storage places where user has to authenticate, storage space makes a strong point of reference [23]. If we take the case of sensor nodes, they have a small amount of memory; hence there we can’t deal with high computation operations [26]. Hence, less the Password Storage Space required less will be resources required.

- Authentication Time- It refers to the time taken by the users to login successfully
- Response Time- In case of responsive process, it is the time taken from issuance of a command to output of that command in that particular process [27].

Efficiency Secondary Indicators

The secondary Indicators are not goals by themselves as they cannot be observed directly; rather they improve the primary indicators. For example, Password composition policies are secondary indicators but they can really help the memorability indicator.

- Password Design – The traditional passwords were prone to many security breaches. So, different alternatives to passwords were designed to overcome the weakness such as System generated passwords, associative passwords, cognitive passwords, passphrases and many more. [4]. Hence, the password design affects the memorability as well as the trust of the user. Password Composition Policies - Rules impose by the system to enable strong passwords creation. Password rules help to enhance the entropy of the password making it hard to guess, which prevent many cases of dictionary as well as exhaustive attack [28]. Hence, the password composition policies should be considered to maintain the trade-off between memorability and security by achieving the maximum memorability, trust, and response time and password storage space.
- Protocols- Finding out our way from the regime of weak to strong authentication, we traversed through the simple transmission to challenge response mechanism. A commonly sought after criteria for selection of authentication measures include: responsiveness, delay, public key, symmetric key, or hash functions, mutual authentication/unilateral authentication, Session key, perfect forward secrecy, and/or anonymity [26]. The prerequisite to the major authentication protocols is cryptography. The most favorable type of protocol is achieved by those using basic cryptographic approaches i.e. symmetric or asymmetric approach. Hash function reduces the computation time, whereas public key infrastructure strengthens the security Ming chuang et.al [29] proposed a transitive relationship based on trust parameter for a lightweight decentralized authentication scheme. The trust parameter is useful for dynamic environment where asymmetric cryptography lacks to improve the performance as well as needs less storage spaces. Hence, the protocol design directly impacts the response time, turnaround time, storage space and the user trust level.
- Context of Use/ Data Attributes- Context Attributes or Situational factors can be described as the context of data interaction of the system with the user. The situational factors are dependent on the situation or the environment in which user is interacting with user. For example, a bank online transaction has completely different environment and attributes as that of a social networking authentication. Elements such as Account Type, Usage Frequency, Key expiry etc. can be thought as Context Attributes. Hence, the data attributes affect the learnability as well as user effort.

CONCLUSION

The current paper tries to segregate the efficiency perspective from the usability attribute in authentication system. Efficiency factor analysis is applied to the password authentication system because it will help to minimize overheads of the resources and will help in values addition of reducing the cost indicating of extra utilities. The proposed efficiency layered model gives a direction of achieving the efficiency goals through the knowledge domains and indicators. The definitions of efficiency were discussed again using this model. The survey for finding out the different problems of authentication, their attributes have taken into account three stakeholders posing different efficiency attributes. We can conclude that; every stakeholder has a different goal of satisfaction because they have different individual attributes. Hence in matter of different situations these different individuals will respond differently. So, an efficient mechanism will be that which efficiently carries out authentication with minimum resource consumption.

REFERENCES

[1] Rengger R, Macleod M, Bowden R, Blaney M, Bevan N. (1993) MUSiC Performance Measurement Handbook. National Physical Laboratory, DITC, Teddington, UK.
[2] Yampolskiy, R.V., 2013. Efficiency theory: A unifying theory for information, computation and intelligence. Journal of Discrete Mathematical Sciences and Cryptography, 16(4-5), pp.259-277.
[3] Jobusch, D.L. and Oldehoeft, A.E., 1989. A survey of password mechanisms: Weaknesses and potential improvements. part 1. Computers & Security, 8(7), pp.587-604.
[4] Kaur, A.A. and Mustafa, K.K., 2019. A Critical appraisal on Password based Authentication. International Journal of Computer Network and Information Security, 11(1), p.47.
[5] Bonneau, J., Herley, C., Van Oorschot, P.C. and Stajano, F., 2012, May. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy (pp. 553-567). IEEE.
[6] Florencio, D. and Herley, C., 2007, May. A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web (pp. 657-666). ACM.
[7] Adams, A. and Sasse, M.A., 1999. Users are not the enemy. Communications of the ACM, 42(12), pp.40-46
[8] Guillaume Desnoës (2015) "How will we manage 200 passwords in 2020?" ITProPortal [online] September 13, 2015, www.itproportal.com/2015/09/13/howwill-we-manage-200- passwords-in-2020/ (Accessed December 16, 2015)
[9] Nielsen, J. (1993), Usability Engineering, Academic Press, London
[10] Quesenbery, W., 2001, October. What does usability mean: Looking beyondease of use'. In Annual conference-society for technical communication (Vol. 48, pp. 432-436).
[11] Quesenbery, W. and Design, W.I., 2003, June. Dimensions of usability: Defining the conversation, driving the process. In UPA 2003 Conference (pp. 23-27).
[12] Quesenbery, W., 2004. Balancing the 5Es of usability. Cutter IT Journal, 17(2), pp.4-11.
[13] Alonso-Ríos, D., Vázquez-García, A., Mosqueira-Rey, E. and Moret- Bonillo, V., 2009. Usability: a critical analysis and a taxonomy. International Journal of Human-Computer Interaction, 26(1), pp.53- 74.
[14] Gupta, D., Ahlawat, A. and Sagar, K., 2014, November. A critical analysis of a hierarchy based Usability Model. In Contemporary Computing and Informatics (IC3I), 2014 International Conference on (pp. 255-260). IEEE.
[15] Morris, R. and Thompson, K., 1979. Password security: A case history. Communications of the ACM, 22(11), pp.594-597.
[16] Shamir, A., 1984, August. Identity-based cryptosystems and signature schemes. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 47-53). Springer Berlin Heidelberg.
[17] Kumar, M., 2004. On the Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards. IACR Cryptology ePrint Archive, 2004, p.163.
[18] Renaud, Karen. "Quantifying the quality of web authentication mechanisms: a usability perspective." Journal of Web Engineering 3.2 (2004): 95-123.
[19] Katz, J., Ostrovsky, R. and Yung, M., 2002, September. Forward secrecy in password-only key exchange protocols. In International Conference on Security in Communication Networks (pp. 29-44). Springer Berlin Heidelberg.
[20] Qian, H., Gong, J. and Zhou, Y., 2012. Anonymous password□based key exchange with low resources consumption and better user□friendliness. Security and Communication Networks, 5(12), pp.1379-1393
[21] Sollins, K.R., 1988, April. Cascaded authentication. In Security and Privacy, 1988. Proceedings., 1988 IEEE Symposium on(pp. 156-163). IEEE
[22] Zviran, M. and Haga, W.J., 1999. Password security: an empirical study. Journal of Management Information Systems, 15(4), pp.161- 185.

[23] Clarke, N.L. and Furnell, S.M., 2007. Authenticating mobile phone users using keystroke analysis. International Journal of Information Security, 6(1), pp.1-14.
[24] Paans, R., & Herschberg, I. S. (1987). Computer security: The long road ahead. Computers & Security, 6(5), 403–416.
[25] Avarne S., How to Find Out a Password, Data Processing & Communication Security, 12,2, (Spring, 1988), 16-17
[26] Kaur, A. and Mustafa, K., 2016, March. Qualitative assessment of authentication measures. In Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on (pp. 694-698). IEEE..
[27] Silberschatz, A., Peterson, J.L. and Galvin, P.B., 1988. Operating system concepts (No. 04; QA76. 76. O63, S5.). New York: Addison- Wesley.
[28] Weir, M., Aggarwal, S., Collins, M. and Stern, H., 2010, October. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proceedings of the 17th ACM conference on Computer and communications security (pp. 162-175). ACM
[29] Chuang, M.C. and Lee, J.F., 2014. TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks. IEEE systems journal, 8(3), pp.749-758
[30] Hartson, H.R., 1998. Human–computer interaction: Interdisciplinary roots and trends. Journal of Systems and Software, 43(2), pp.103-118.
[31] Van Welie, M., Van Der Veer, G.C. and Eliëns, A., 1999, September. Breaking Down Usability. In Interact (pp. 613-620).
[32] Shneiderman, B. (1998), Designing the User Interface, Addison- Wesley Publishing Company, USA
[33] Luczak, H. (1997). Task analysis. In G. Salvendy (Ed.), Handbook of human factors and ergonomics (2nd ed., pp. 340-416). New York: Wiley
[34] Proctor, R.W., Lien, M.C., Salvendy, G. and Schultz, E.E., 2000. A task analysis of usability in third-party authentication. Information Security Bulletin, 5(3), pp.49-56.