A NOVEL APPROACH TOWARDS INTRUSION DETECTION AND PREVENTION AGAINST STOLEN PASSWORDS THROUGH KEYSTROKE ANALYSIS

Dr. Kunal Gupta,
IT Department, Higher College of Technology, Muscat, Sultanate of Oman
kunal.gupta@hct.edu.om

Dr. Mohammed Said Sulaiman Al- Bahri,
IT Departement, Higher College of Technology, Muscat, Sultanate of Oman
mohammed.albahri@hct.edu.om

ABSTRACT

Our Research revolves around the idea that a secure add-on authentication mechanism can ensure, that even if a password is stolen, it cannot be utilized in order to access a system. In fact, whenever the stolen credentials are used to try gain access of a system, the mechanism will not only stop the intruder from gaining the access, it will also alert the owner of the account that his account has been compromised, the attempt to access his account has been made, and he should try to change his password to block any such attempt in the future.

Keywords: *Intrusion, Password, keystoke analysis, authentication*

1. INTRODUCTION

The current era, the era of Information Technology, dictates that information is everything. Privacy governs that information is shared in an authorized manner, and authentication controls provides the basis of imposing such a control. Authentication mechanisms themselves have gone through a variety of changes in the past decade, from two factor authentication, which requires the user to provide additional information other than the passwords for identifying themselves, to biometric system, where an intrinsic property of the user is taken into account to prove one's identity. The biometric mechanisms ensures that an individual identity is proven through his biological properties[1], but being relatively expensive due to the hardware costs and physical deployment/ mobility issues, cannot be employed everywhere. So the username and password still remains the major mechanism as far as authentication services are concerned.The password being the secret information becomes the target of the attacker all around the world. Hackers have developed several methods to steal passwords, which include password guessing, password cracking, dictionary attacks, social engineering attacks and many more. Strong password policy is enforced by many organizations, which has proven to be effective against several kind of attacks. But the stringent requirements of a strong password policy has again provided with some bottleneck.

People are forced to choose passwords that are lengthy, contains complex elements, and use of words, names and personal information is advised against usage. This makes the passwords difficult to remember, especially for the non-technical users. They either don't follow theguidelines or record their passwords on paper or files and keep them at an accessible place, which again makes the task of the attacker to obtain the password much easier.

Our novel approach gives the user, freedom from remembering complex passwords, choosing a password that can contain personal information, yet provides them the security that is always desired – namely, even if the password falls into the hands of an intruder, it cannot be used for accessing one's system.

2. METHOD

Our previous research [2], we focussed on the unique features of keystroke values[3], which were recorded for each character typed for a given password, in form of seconds. The results of the implementation of our algorithm yielded a result of approximately, 88.8% correctness. The algorithm was devised with reference to [4][5].

This research takes our previous research further to devise a novel method to provide an intrusion detection and prevention method for stolen passwords.

3. FRAMEWORK

Our research led down to the following framework which takes user input for username and password. The password if matched against the values stored in database, activates the add on authentication services provided by our framework. The framework checks the keystroke values, in terms of time, and matches with the threshold values stored in the database. If a match is found then the user is granted access and the threshold values are adjusted according to the new keystroke values entered by the user. If the threshold values are violated, then the two factor authentication method is activated, and the user is asked for additional information. If the user does not provides the additional authentication information within the speculated time, then the genuine user whose credentials are being used is notified immediately of the attempt to break into the system, and the access is blocked. If the user however, provides his additional authentication information, the system is assured of the genuineness of the user and the access is granted; the threshold values are also adjusted if the variation is within the predefined agreed variation values. If the user provides the additional authentication that is incorrect, the system is able to realize that the information is being

accessed by an intruder and blocks the access to the system thereafter for that request, and sends an alert to the genuine user of his password being compromised, and the account access is attempted by an intruder. The access has been blocked and he is advised to change his password at the earliest, as his password is stolen.

The framework provides a basis for adopting an intelligent and adaptive framework that not only ensures that an intruder cannot access the system even if the credentials are compromised, it also acts as an alerting mechanism for the user to advise him to change his password as his credentials are known to someone else.

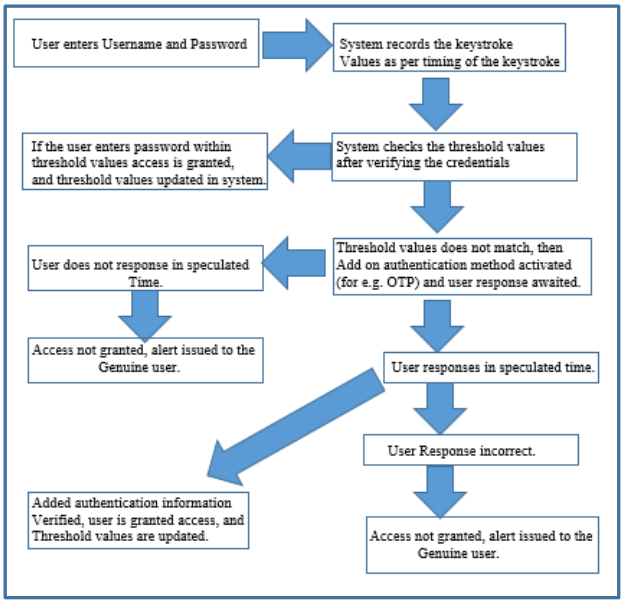

Fig. 1: Framework for the Intrusion Detection and prevention mechanism for authentication using Keystroke Analysis

4. CONCLUSION

The above framework can be duly deployed for desktop system all across the world as even in this era of smart phones, desktop computers provide an important means of information gathering and processing tool. The above system deployment will ease down the stringent requirements of a strong password policy, and reduce the account recovery process. Not only the stolen credentials will be difficult to be taken advantage of, once stolen and attempted to used, they will be notified to the user.

5. REFERENCES

[1] F. Monroseand A. D. Rubin, "Keystroke dynamics as a biometric for authentication," in Future Generation Computer Systems, vol. 16, issue 4, pp. 351-359, February 2000.

[2] Kunal Gupta, Brijesh Jajal, "Securing Password Through Keystroke Forensic", in Journal of Multidisciplinary Engineering Science and Technology (JMEST), June, 2016.

[3] A.Guvenand I. Sogukpinar, "Understanding users' keystroke patterns for computer access securifity," in Computers & Security, vol. 22, issue 8, pp. 695-706, December 2003.

[4]M. Karnan, M. Akila and N. Krihnaraj, "Biometric personal authentication using keystroke dynamics: A review," in Applied Soft computing, vol. 11, issue 2, pp. 1565-1573, March 2011.

[5] P. Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation," in Information Security Technical Report, vol. 17, issue 1-2, pp. 36-43, February 2012.