CHAPTER 1

INDTRODUCTION

This chapter discusses the research rationale which consists of the background and followed with an overview of several previous methods. The discussion continues with the theoretical framework, the conceptual framework, the statement of the problem, hypothesis, assumption, scope, and delimitation, as well as the importance of the studies

1.1 Rationale

Authentication using a username and password has been used universally by most applications but does not guarantee that the user involved authentication is the right user, so it is possible to attack by imitating it. The attack is called spoofing. Some systems require the use of long password and need to be changed frequently to prevent spoofing. That may be difficult to remember, create and manage [8]. Behavior is a unique component that can be used to continuously observe user behavior, in this case it is used for continuous user authentication.

The movement of mouse, how a user typing for searches and selects information can be used as unique behavioral and produces a stable behavior pattern. Although these approaches do not require special hardware but require the installation of specialized software to monitoring users [7] [4]. Leslie Milton [7] proposed a study to verify by looking at user behavior based on web logs. Using a web log to model users in accessing the same session produces 45% accuracy, which means it is still vulnerable against spoofing attacks.

Spoofing is considered dangerous, because it can increase the risk of counterfeiting during the authentication process. With a web log component that records user activity, spoofing can be minimized, because users have unique habits when accessing the system. Therefore web log components can be used for continuous authentication.

The CUA has been thoroughly assessed using biometrics. In one study, fingerprints were used to measure computational behavior using computational linguistics and structural semantic analysis [2]. The survey uses a combination of indicators, including eye scans and keystrokes, to evaluate how users search for and select information. In addition, some CUA studies use one or more hard and soft biometric data for persistent user authentication. Niinuma et al. Proposed a CUA scheme to automatically register the color of a user's clothing and face as a subtle biometric feature [10] [11]. The results of this study indicate that systems that successfully authenticate users have high resistance to user attitudes. A limitation of this study is that additional hardware is required to implement this approach, which can become expensive if the entire organization uses this feature for user authentication.

Monrose et al. Propose an unambiguous user identification method based on keystroke analysis [8]. Your writing dynamics focus on how you write, not what you write. The user's habitual typing rhythm depends on the user and his environment. Thus, the limitations of this approach arise when users are faced with environmental factors that affect their typing. Altinok et al. Propose a continuous biometric authentication system that provides an evaluation of authentication credibility at any time, even in the absence of biometric data [1]. In this case, the validation uncertainty increases over time, leading to a decrease in the usability of the system. In a similar study by Kang et al. presents temporary integration of biometric and behavioral features for permanent user authentication [5].

Face tracking systems use color and contour information that is used to calculate behavioral characteristics. Shen et al. Use mouse dynamics for continuous user authentication [12]. This method is used to monitor mouse activity to detect intruders. However, there are some limitations to this new approach. Changes in behavior occur due to human or environmental factors. For example, if a user changes the development environment or undergoes biological or emotional changes, the user's behavior will change dramatically. Such changes may identify users as fraudulent.

Xie et al. Apply a critical approach for early identification of authorized users when using online services by carrying out a verification process without using biometric data [14]. They implemented the Souche system to track confirmations via social communities (i.e. Twitter, email). Souche managed to identify 85% of legitimate users and block intruders. Our research aims to solve these problems without the presence of a social community. In recent years, mobile devices have been used to study user behavior. Researchers introduced SenSec as a mobile platform to collect sensory data to build a traffic model of user interaction with mobile devices [15]. As in our work, n-grams are used to capture non-standard samples. The SenSec system achieves over 70% accuracy in user authentication and classification tasks. Furthermore, Saevanee et al. The use of multi-template biometric methods with mobile devices uses language profiles, keystroke dynamics, and behavior profiles to authenticate users [1]. The results of this study showed that annoying authentication requests were reduced by 91%.

1.2 Theoretical Framework

The weblog component can be used to define user habits. In internet systems, and more specifically e-commerce, the system records user actions from logging in to logging out. Based on this action, this user procedure will be used to authenticate the user. Given that these user habits cannot be faked and are unique, user habits can be used as user characteristics.

1.3 Conceptual Framework/Paradigm

Due to user characteristics, habits or behaviors can be used appropriately to authenticate users.

This behavior-based authentication method can be achieved by observing a sequence of behaviors or by observing dominant habits over time. Based on the observations, the time characteristics of the user can be obtained, for example, User A usually opens the basket in the morning. This feature is then used to authenticate the user. By using this feature, intruders will be more difficult to hack this feature because it will be difficult to show someone's habits.

1.4 Statement of the Problem

Leslie et al [7].observed the behavior of access to the military web system to strengthen the behavior-based authentication method, proposed using the path. Military weblogs are very specific, so they need to be made more general. For that we take datasets not from the military. But we take the more general example of e commerce. However, our method can actually be used by other environments such as schools, government, etc. However, with path alone this method has a weakness, namely that this method only identifies users based on their roles. Meanwhile, there is currently a great need for a system that can identify users based on their identities

Therefore, it can be concluded that the method proposed by Leslie et al. only focuses on the path to identify the user's role, can't identify the user based on their identity.

1.5 Objective and Hypotheses

The purpose of the proposed method is to identify users based on their identities in an e-commerce system, using weblogs that are recorded on the system when users interact in the system, by utilizing several user attributes such as, user id, event type, category, and product id.

By adding these attributes, the method for identifying users based on behavior can be improved because these attributes increase the accuracy of behavior pattern-based features.

1.6 Assumption

Every registered or login user will separate if their behaviour recording not same with last login, system will send a confirmation email, and user can show old behaviour flow (ex. How many access, what time usually access). Not every user have constant activity, we will modeling user who have minimum requirement model. Minimum requirement model

is user who have activity at last 2 days with constant activity, or user have data training at last 18 - 30 days

1.7 Scope and Delimitation

The scope of this research is to increase the security of ecommerce authentication method by adding additional user attribute. The result of the proposed method is a user behaviour based feature/biometric.

1.8 Significance of the Study

The proposed method is based on the user behavior which is difficult to spoof thus the authentication method is stronger then Leslie's method[7]