International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

Behavioral Biometrics for Human Computer Interaction

P. L. Ramesh[1], Shamim[2] and Bharathi Devi Patnala[3]

[1]*HOD Dept of Computer Science K.B.N College Vijayawada*
[2]*Asst Professor, Dept. of M.Sc (CS), K.B.N PG College, Vijayawada*
[3]*Asst Professor Dept of MCA K.B.N PG College Vijayawada*

Abstract— Human Computer Interaction (HCI) explores how human beings interact with computational devices. This type of interaction, relatively unique to every computer user can be analyzed to develop a non-intrusive authentication mechanism Direct HCI biometrics are based on abilities, style, preference, knowledge, or strategy used by people while working with a computer. The indirect HCI-based biometrics is events that can be obtained by monitoring users' HCI behavior indirectly via observable low-level actions of computer software. HCI-based biometrics provides a number of advantages over traditional biometric technologies. After comparing accuracy rates for verification of users using different HCI-based biometric approaches we address privacy issues which arise with the use of HCI dependent biometrics. Finally, we present results of our experiments with direct and indirect HCI-based behavioral biometrics employed as a part of an intrusion detection system

Index Terms— Behavioral biometrics, Human Computer Interaction, Intrusion Detection

I. INTRODUCTION

In the context of authentication, biometrics have several advantages over traditional authentication techniques that verify identity based on something one knows (e.g. a password) or something one has (e.g. a hardware token). In particular, biometrics cannot be forgotten, stolen, or misplaced. Additionally, HCI-based behavioral biometrics have the advantage that they are less obtrusive than other biometrics and do not require special hardware in order to capture the necessary biometric data HCI-based biometrics are usually only briefly mentioned and only those which are in large part based on muscle control such as keystrokes, or mouse dynamics are well researched. HCI-based biometrics provide a number of advantages over traditional biometric technologies. They can be collected non-obtrusively or even without the knowledge of the user. Collection of data usually does not require any special hardware and is so very cost effective. While HCI-based biometrics are not unique enough to provide reliable human identification they have been shown to provide high accuracy identity verification. In their interaction with computers human beings employ different strategies, use different style and apply unique abilities and knowledge. Intrusion detection researchers attempt to quantify such HCI-based-biometric traits and use resulting feature profiles to successfully verify user identity and reject intruders. HCI-based biometrics can be subdivided into two different categories known as direct and indirect HCI-based biometrics.

First group is made up of those biometrics which are based on direct human interaction with input devices such as keyboard, computer mouse, which rely on supposedly innate, unique and stable muscle actions and those biometrics which are based on advanced human behavior such as strategy, knowledge or skill exhibited by the user during interaction with different software. Examples of such high level HCI-based behavioral biometrics include: email behavior, programming style, utilized online game strategy, biometric sketch, and command line lexicon.

The second group consists of the indirect HCI-based biometrics which are events that can be obtained by monitoring user's HCI behavior indirectly via observable low-level actions of computer software, those include audit logs, call-stack data, GUI interaction, network traffic, registry access, storage activity, and system calls. These low-level events are produced unintentionally by the user during interaction with different software applications during pursuit of some, potentially mischievous, high level goals.

II. DIRECT HCI-BASED BIOMETRICS

In this section we present an overview of the most established Direct Human Computer Interaction-Based Biometrics (DHCIBB). DHCIBB can be subdivided into two different categories, first one consisting of human interaction with input devices such as keyboards, mice, and haptics which rely on supposedly innate, unique and stable muscle actions. The second group consists of HCI-based behavioral biometrics which measure advanced human behavior such as strategy, knowledge or skill exhibited by the user during interaction with different software

Keystroke Dynamics: Typing patterns are characteristic to each person, some people are experienced typists utilizing the touch-typing method, and others utilize the hunt-and-peck approach which uses only two fingers. Those differences make verification of people based on their typing patterns a proven possibility, some reports suggest identification is also possible. For verification a small typing sample such as the input of user's password is sufficient, but for recognition a large amount of keystroke data is needed and identification is based on comparisons with the profiles of all other existing users already in the system. Keystroke features are based on time durations between the keystrokes, inter-key strokes and dwell times, which is the time a key is pressed down, overall typing speed, frequency of errors (use of backspace), use of numpad, order in which user presses shift key to get capital letters and possibly the force with which keys are hit for specially equipped keyboards. Keystroke dynamics is probably the most researched type of HCI-based biometric, with novel research taking place in different languages, for long text samples, and for email authorship identification.

Mouse Dynamics: By monitoring all mouse actions produced by the user during interaction with the Graphical User Interface (GUI), a unique profile can be generated which can be used for user re-authentication. Mouse actions of interest include general movement, drag and drop, point and click, and stillness. From those a set of features can be extracted for example average speed against the distance traveled, and average speed against the movement direction. Pusara et al. describe a feature extraction approach in which they split the mouse event data into mouse wheel movements, clicks, menu and toolbar clicks. Click data is further subdivided into single and double click data tried to improve accuracy of mouse-dynamics-based biometrics by restricting the domain of data collection to an online game instead of a more general GUI environment. As a result applicability of their results is somewhat restricted and the methodology is more intrusive to the user. The system requires around 10-15 minutes of devoted game play instead of seamless data collection during the normal to the user human computer interaction. As far as the extracted features, x and y coordinates of the mouse, horizontal velocity, vertical velocity, tangential velocity, tangential acceleration, tangential jerk and angular velocity are utilized with respect to the mouse strokes to create a unique user profile.

III. INDIRECT HCI-BASED BIOMETRICS

Indirect HCI-based biometrics are sometimes known to different researchers under different names. IDS based on system calls or audit logs are often classified as utilizing program execution traces and those based on call-stack data as based on system calls. The confusion is probably caused by the fact that a lot of interdependency exists between different indirect behavioral biometrics and they are frequently used in combinations to improve accuracy of IDS being developed. For example system calls and program counter data may be combined in the same behavioral signature or audit logs may contain information about system calls. Also we can't forget that a human intruder is indirectly behind each one of those reflections of behavior and so a large degree of correlation is to be expected. In this section we tried to distill all indirect HCI-based biometrics into the seven well defined groups, but some overlay undoubtedly exists

IV. COMPARISON AND ANALYSIS

All of the presented direct HCI-based biometrics share a number of characteristics and so can be analyzed as a group using seven properties of good biometrics presented by Jain et al. [1, 5].

Universality HCI-based biometrics are dependent on specific abilities possessed by different people to a different degree or not at all and so in a general population universality of HCI-based biometrics is very low. But since HCI-based biometrics are only applied to those who participate in computer interactions, actual universality of styles, different online game strategies and varying preferences are only sufficient for user verification not identification unless the set of users is extremely small.

Permanence HCI-based biometrics exhibit a low degree of permanence as they measure behavior which changes with time as person learns advanced techniques and faster ways of accomplishing tasks. However, this problem of concept drift is addressed in the behavior based intrusion detection research and systems are developed capable of adjusting to the changing behavior of the users

Collectability Collecting HCI-based biometrics is relatively easy and unobtrusive to the user. In some instances the user may not even be aware that data collection is taking place. The process of data collection is fully automated and is very low cost.

Performance The identification accuracy of HCI- based biometrics is very low particularly as the number of users in the database becomes large. However verification accuracy can be very good for some HCI-based biometrics. HCI-based biometrics is a 100%.

Uniqueness Since only a small set of different approaches to performing any task on a computer exists uniqueness of HCI-based biometrics is relatively low. Number of existing programming.

Behavioral Comparison

Behavioral patterns are detected from a stream of mouse events at the feature level. Various algorithms have been used in the literature to detect and compare behavioral patterns. These range from simple distance metrics to complex machine learning algorithms like neural network

Like other biometric authentication systems, those based on mouse dynamics are typically evaluated with respect to the following metrics:

False Acceptance Rate (FAR)–the probability that the system will incorrectly label the active user as the same user that produced the enrollment signature.

False Rejection Rate (FRR)–the probability that the system will incorrectly label the active user as an impostor, when in fact it is not.

Equal Error Rate (EER)–the error rate when the system's parameters (such as the decision threshold) are set such that the FRR and FAR are equal. The lower the EER the more accurate the system.

Verification time–the time required by the system to collect sufficient behavioral data to make an authentication decision.

Software Interaction Based Biometrics

Email Behavior: Email sending behavior is not the same for all individuals. Some people work at night and send dozens of emails to many different addresses; others only check mail in the morning and only correspond with one or two people. All this peculiarities can be used to create a behavioral profile which can serve as a behavioral biometric for an individual. Length of the emails, time of the day the mail is sent, how frequently inbox is emptied and of course recipients' addresses among other variables can all be combined to create a baseline feature vector for the person's email behavior.

Programming Style:

With the increasing number of viruses, worms, and Trojan horses it is often useful in a forensic investigation to be able to identify an author of such malware programs based on the analysis of the source code. It is also valuable for the purposes of

software debugging and maintenance to know who the original author of a certain code fragment was. Spafford et al. [22] have analyzed a number of features potentially useful for the identification of software authorship. In case only the executable code is available for analysis, data structures and applied algorithms can be profiled as well as any remaining compiler and system information, observed programming skill level, knowledge of the operating system and choice of the system calls. Additionally use of predefined functions and provisions for error handling is not the same for different programmers.

Computer Game Strategy: Ramon et al.have demonstrated possibility of identifying Go players based on their style of game play. They analyzed a number of Go specific features such as type of opening moves, how early such moves are made and total number of liberties in the formed groups. They also speculate that the decision tree approach they have developed can be applied to other games such as Chess or Checkers.

Biometric Sketch: Bromme et al. [28, 29] proposed a biometric sketch authentication method based on sketch recognition and a user's personal knowledge about the drawings content. The system directs a user to create a simple sketch for example of three circles and each user

is free to do so in any way he pleases. Because a large number of different combinations exist for combining multiple simple structural shapes sketches of different users are sufficiently unique to provide accurate authentication. The approach measures users' knowledge about the sketch, which is only available to the previously authenticated user. Such features as the sketches location and relative position of different primitives are taken as the profile of the sketch. Similar approaches are tried by Varenhorst with a system called Passdoodles and also by Jermyn et al.with a system called Draw-a- Secret. Finally a V-go Password requests a user to perform simulation of simple actions such as mixing a cocktail using a graphical interface, with the assumption

V. CONCLUSION

Reliable computer security to a large degree depends on development of biometric technology in general and HCI-based biometrics in particular. This affordable and non-intrusive way of verifying the user's identity holds a lot of potential to developing secure and user friendly systems and networks. As long as the issues of privacy are sufficiently addressed by the developers of HCI-based security systems commercial potential of development in this area is very substantial.In addition to computers, HCI-based biometrics are also well suited for verification of users which interact with cell phones, smart cars, or points of sale terminals. As the number of electronic appliances used in homes and offices increases so does the potential for utilization of this novel and promising technology. Also inclusion of additional input devices such as stylus, touch-pad, and digitizing tablet in the scope of HCI-based biometrics research will make the technology more applicable for the general public. Future research should be directed at increasing overall accuracy of such systems as well as looking into possibility of developing multimodal HCI- based biometrics as people often engage on multiple channels of interaction with a computer, for example using a mouse and keyboard simultaneously

VI. REFERENCES

[1] K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst., Vol. 14., pp. 4-20, Video Technol,2004.

[2] R. V. Yampolskiy, "Motor-Skill Based Biometrics," In Assuring Business processes, Proceedings of the 6th Annual Security Conference, Ed. G. Dhillon. Global Publishing, Las Vegas, NV, USA., April 11-12, 2007.

[3] R. V. Yampolskiy, "Human Computer Interaction Based Intrusion Detection," 4th International Conference on Information Technology: New Generations (ITNG 2007), Las Vegas, Nevada, USA, April 2-4, 2007.

[4] J. Ilonen, "Keystroke dynamics," Available at:www.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf, Retrieved July 12, 2006.

[5] A. K. Jain, R. Bolle, and S. Pankanti, "BIOMETRICS: Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.

[6] F. Monrose and A. D. Rubin, "Keystroke Dynamics as a Biometric for Authentication," Future Generation Computing Systems (FGCS) Journal: Security on the Web (special issue), March 2000.

[7] F. Bergadano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," ACM Transactions on Information and System Security (TISSEC), November 2002.

[8] D. Gunetti, C. Picardi, and G. Ruffo, "Keystroke Analysis of Different Languages: a Case Study," Proc. of the Sixth Symposium on Intelligent Data Analysis (IDA 2005), Madrid, Spain, 2005.

[9] M. Curtin, C. C. Tappert, M. Villani, G. Ngo, J. Simone, H. S. Fort, and S. Cha, "Keystroke Biometric Recognition on Long-Text Input: A Feasibility Study," Proc. Int. Workshop Sci Comp/Comp Stat (IWSCCS 2006), Hong Kong, June 2006.