Human Computer Interaction Based Intrusion Detection

Roman V. Yampolskiy
Center for Unified Biometrics and Sensors and IGERT in GIS
rvy@buffalo.edu

Abstract

In this paper we survey the state of the art in human computer interaction based biometrics which are based on abilities, style, preference, knowledge, or strategy used by people while working with a computer. We examine current research and analyze the types of features used to describe HCI behavior. 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 dependant biometrics. Finally, we present results of our experiments with behavior-based intrusion detection in online game networks based on the strategy utilized by the players.

1. Introduction

With the proliferation of computers and of the Internet in our every day lives need for reliable computer security steadily increases. Research in biometric technologies offers one of the most promising approaches to providing user friendly and reliable control methodology for access to computer systems and networks. Majority of such research is aimed at studying well established physical biometrics such as fingerprint or iris scans [24]. 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. 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. In this paper we concentrate on reviewing and analyzing all existing HCI-based biometric technologies.

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.

2. HCI-Based Biometrics

In their everyday interaction with computers human beings employ different strategies, use different style and apply unique abilities and knowledge. HCI-based-biometrics researchers attempt to quantify such traits and use resulting feature profiles to successfully verify identity. In this section we present an overview of the most established HCI-based biometrics. HCI-based biometrics 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 [8]. 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. Additional methods exist that rely on monitoring a user's HCI behavior indirectly [38], those include monitoring system call traces [11], audit logs [21], program execution traces [16], registry access [4], storage activity [36], and call-stack data analysis [12], but those approaches are beyond the scope of this paper.

2.1. Input Device Interaction Based Biometrics

2.1.1. 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 [22]. 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 [22, 23]. Keystroke dynamics is probably the most researched type of HCI-based biometric [33, 6], with novel research taking place in different languages [19], for long text samples, [9, 5] and for email authorship identification [20].

International Conference on Information Technology (ITNG'07)
0-7695-2776-0/07 $20.00 © 2007

2.1.2. 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 [38]. 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 [2, 1]. Pusara et al. [38] 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.

Gamboa et al. [14, 15] have 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.

2.1.3. Haptic Haptic systems are computer input/output devices which can provide us with information about direction, pressure, force, angle, speed, and position of user's interactions [34, 35]. Because so much information is available about the user's performance a high degree of accuracy can be expected from a haptic based biometrics system. Orozco et al. [34, 35] have created a simple haptic application built on an elastic membrane surface in which the user is required to navigate a stylus through the maze. The maze has gummy walls and a stretchy floor. The application collects data about the ability of the user to navigate the maze, such as reaction time to release from sticky wall, the route, the velocity, and the pressure applied to the floor. The individual user profiles are made up of such information as 3D world location of the pen, average speed, mean velocity, mean standard deviation, navigation style, angular turns and rounded turns.

In a separate experiment Orozco et al. [45] implement a virtual mobile phone application where the user interacts through a haptic pen to simulate making a phone call via a touch pad. The keystroke duration, pen's position, and exerted force are used as the raw features collected for user profiling.

2.2. Software Interaction Based Biometrics

2.2.1. 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. Some work in using email behavior modeling was done by Stolfo et al. [43, 44]. They have investigated possibility of detecting virus propagation via email by observing abnormalities in the email sending behavior, such as unusual clique of recipients for the same email. For example sending the same email to your girlfriend and your boss is not an everyday occurrence.

De Vel et al. [48] have applied authorship identification techniques to determine the likely author of an email message. Alongside the typical features used in text authorship identification such as count of function-words and word length frequency distribution authors also used some email specific structural features such as: use of a greeting, farewell acknowledgment, signature, number of attachments, position of re-quoted text within the message body, HTML tag frequency distribution and total number of HTML tags. Overall, almost 200 features are used in the experiment, but some frequently cited features used in text authorship determination are not appropriate in the domain of email messages due to the shorter average size of such communications.

2.2.2. 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. [42] 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.

In case the original source files are available a large number of additional identifying features become accessible such as: chosen programming language, code formatting style, type of code editor, special macros, comment style, variable names, spelling and grammar, use of language features such as choice of loop structures, the ratio of global to local variables, temporary coding structures, and finally types of mistakes observable in the code. Software metrics such as number of lines of code per function, comment-to-code ratio and function complexity may also be introduced [42]. Similar code features are discussed by Gray et al. [18] and in Grantzeskou et al. [13].

2.2.3. Computer Game Strategy Ramon et al. [39] 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.

Jansen et al. [25] report on their research in chess strategy inference from game records. In particular they were able to surmise good estimates of the weights used in the evaluation function of computer chess players and later applied same techniques to human grandmasters. Their approach is aimed at predicting future moves made by the players, but the opponent model created with some additional processing can be utilized for opponent identification or at least verification. This can be achieved by comparing new moves made by the player with predicted ones from models for different players and using the achieved accuracy scores as an indication of which profile models which player.

2.2.4. Biometric Sketch Bromme et al. [7, 3] 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 [47] with a system called Passdoodles and also by Jermyn et al. [26] 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 that all users have their unique approach to bartending [40].

2.2.5. Command Line Lexicon A popular approach to the construction of behavior based intrusion detection systems, is based on profiling the set of commands utilized by the user in the process of interaction with the operating system. A frequent target of such research is UNIX operating system, probably due to it having mostly command line nature. Users differ greatly in their level of familiarity with the command set and all the possible arguments which can be applied to individual commands. Regardless of how well a user knows the set of available commands; most are fairly consistent in their choice of commands used to accomplish a particular task.

A user profile typically consists of a list of used commands together with corresponding frequency counts, and lists of arguments to the commands. Data collection process is often time consuming since as many as 15,000 individual commands need to be collected for the system to achieve high degree of accuracy [41, 32]. Additional information about the secession may also be included in the profile such as the login host and login time, which help to improve accuracy of the user profile as it is likely that users perform different actions on different hosts [10]. Overall, this line of research is extremely popular [51, 31, 29, 30], but recently a shift has been made towards user profiling in a graphical environment such as Windows as most users prefer convenience of a Graphical User Interface (GUI). Typical features extracted from the user's interaction with a windows based machine include: time between windows, time between new windows, number of windows simultaneously open, and number of words in a window title. [17, 27].

3. Comparison and Analysis

All of the presented 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. [23, 24].

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 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 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 [28, 46].

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.

Acceptability Since HCI-based biometrics can be collected without user participation they enjoy a high degree of acceptability, but might be objected to for ethical or privacy reasons.

Circumvention It is relatively difficult to get around HCI-based biometric systems as it requires intimate knowledge of someone else's behavior, but once such knowledge is available fabrication might be very straightforward. This is why it is extremely important to keep the collected user profiles securely encrypted.

While many HCI-based biometrics are still in their infancy some very promising research has already been done. The results obtained justify feasibility of using human computer interaction for verification of individuals and further research in this direction is likely to improve accuracy of such systems. Table 1 summarizes obtained accuracy ranges for the set of HCI-based biometrics for which such data is available.

HCI Biometric	**Verification Accuracy Range**
Keystroke Dynamics [22, 23, 19, 9, 5, 20]	94.7-100%
Email Behavior [43, 44, 48]	86.2-90.5%
Mouse Dynamics [38, 2, 1, 14, 15]	98.25-100%
Haptic [34, 35, 45]	49.0-79.8%
Computer Game Strategy [49, 50, 39]	53.0-78.33%
Biometric Sketch [7, 3]	98.7-100.0%
Command Line Lexicon [41, 32, 10, 51, 31, 29, 30]	66.0-99.0%

Table 1: Reported verification accuracy for HCI biometrics

4. Ethical and Privacy Issues

Because HCI-based biometrics measure our personal traits any data collected in the process of generation of a user profile needs to be safely stored in an encrypted form. An additional property of HCI-based profiles is that they might contain information which might be of interest to third parties which might discriminate against individuals based on such information. As a consequence intentionally revealing or obtaining somebody else's biometric profile for the purposes other than verification would be highly unethical. Examples of private information which might be revealed by some HCI-based biometric profiles follow:

Keystroke Dynamics May indicate that an individual is physically challenged or less seriously has a poor typing techniques and is so an inefficient employee.

Haptics Similarly to keystroke dynamics and mouse dynamics may reveal motor control problems of a particular user.

Email Behavior An employer would be interested to know if employees send out personal emails during office hours.

Programming Style Software metric obtained from analysis of code may indicate a poorly performing coder and as a result jeopardize the person's employment.

Computer Game Strategy If information about game strategy is obtained by the player's opponents it might be analyzed to find weaknesses in the player's game and as a result be financially costly.

Command Line Lexicon Information about proficiency with the commands might be used by an employer to decide if you are sufficiently qualified for a job involving computer interaction.

5. Experiments

We have developed a methodology for treating the strategy used while playing a game as a type of a behavioral biometric. The game of poker was used as an example of a game with a clearly identifiable player strategy. A profile signature produced for each player was used as the person's behavioral biometric profile. This approach can be utilized by online casinos to detect a hacker who is using a stolen account. This is currently a major problem in the world of online game networks and a successful solution can be beneficial not just from theoretical but also from a practical point of view.

First a user profile is generated either by data mining an existing database of poker hands or by observing a live game of poker. To study the strategy of poker players scientifically, we needed to quantify and statistically analyze their behavior. In order to do so we defined a number of variables associated with actions of poker players. The parameters chosen were selected because they can be easily tracked by relatively straightforward methodologies and more importantly they are believed to accurately describe the long-term model of player's behavior for poker [49, 50].

The profile consists of frequency measures indicating range of cards considered by the player at all stages of the game. It also measures how aggressive the player is via such variables as percentages of re-raised hands. The profile is actually human readable meaning that a poker expert can analyze and understand strategy employed by the player from observing his or her behavioral profile [37]. Table 2 demonstrates a sample profile for a player named Bob.

Player Name: Bob			Hands Dealt: 224	
	Pre-Flop	Flop	Turn	River
# of Hands	224	68	46	33
Folded	67%	28%	24%	18%
Checked	7%	54%	52%	52%
Called	21%	32%	28%	33%
Raised	4%	1%	4%	6%
Check-Raised	0%	4%	0%	0%
Re-Raised	0%	1%	0%	0%
All-In	1%	3%	4%	39%

Table 2: A sample strategy based behavioral profile [50]

In the Table 2 we see a 24 dimensional feature vector (number of hands played is only used to determine if we have enough information to put confidence in our statistical profile and is not counted as a part of a profile) [50].

Next, a similarity measure is obtain between the feature vector generated based on the recently collected player data and the data for the same player obtained in previous sessions. A score is generated indicating how similar the current style of play is to the historically shown style of play for a particular player. If a score is above a certain threshold, it might indicate that a different user from the one who has originally registered is using the account and so the administrator of the network needs to be alerted to that fact. If the score is below some threshold, the system continues collecting and analyzing the player data. We used Euclidian Distance as a similarity measure in our implementation [49, 50].

For the user verification experiment a databank of 30 player signatures each one was compared with one profile taken from the same player as the one who generated the original signature and with another profile taken from a randomly chosen player. Giving us an experimental set up in which intruders and legitimate users are equal in number. Using our similarity measure and a threshold of 75 the algorithm has positively verified 46.66% (28) users. The False Accept Rate (FAR) was 13.33% (8 users) and False Reject Rate (FRR) was only 8.33% (5 users). This gives us player verification with overall 78.33% accuracy. The value of the threshold is not a universal constant and depends most of all on the maximum FRR and FAR, which can be tolerated by the application. Additional factors such as the similarity function used and the structure and size of the behavioral signature utilized also influence the choice of the optimal threshold value [49, 50].

6. Conclusions

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.

7. References

[1] A. A. E. Ahmed and I. Traore, *Anomaly Intrusion Detection based on Biometrics*, *Workshop on Information Assurance*, United States Military Academy, West Point, NY, June 2005.

[2] A. A. E. Ahmed and I. Traore, *Detecting Computer Intrusions Using Behavioral Biometrics*, *Third Annual Conference on Privacy, Security and Trust*, St. Andrews, New Brunswick, Canada, October, 2005.

[3] S. Al-Zubi, A. Brömme and K. Tönnies, *Using an Active Shape Structural Model for Biometric Sketch Recognition*, *In Proceedings of DAGM*, Magdeburg, Germany, 10.-12. September 2003, pp. 187-195.

[4] F. Apap, A. Honig, S. Hershkop, E. Eskin and S. Stolfo, *Detecting malicious software by monitoring anomalous windows registry accesses*, *Technical report, CUCS Technical Report*, 2001.

[5] G. Bartolacci, M. Curtin, M. Katzenberg, N. Nwana, S.-H. Cha and C. C. Tappert, *Long-Text Keystroke Biometric Applications over the Internet*, *MLMTA*, 2005, pp. 119-126.

[6] F. Bergadano, D. Gunetti and C. Picardi, *User authentication through keystroke dynamics*, *ACM Transactions on Information and System Security (TISSEC)*, November 2002, pp. 367-397.

[7] A. Brömme and S. Al-Zubi, *Multifactor Biometric Sketch Authentication*, *In A. Brömme and C. Busch, editors, Proceedings of the BIOSIG 2003*, Darmstadt, Germany, 24. July 2003, pp. 81-90.

[8] Caslon-Analytics, *Available at: http://www.caslon.com.au /biometricsnote6.htm*, Retrieved October 2, 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.

[10] V. Dao and V. Vemuri, *Profiling Users in the UNIX OS Environment*, *International ICSC Conference on Intelligent Systems and Applications*, University of Wollongong Australia, Dec. 11-15, 2000.

[11] D. E. Denning, *An intrusion-detection model*, *IEEE Transactions on Software Engineering*, 1987, pp. 222-232.

[12] H. H. Feng, O. M. Kolesnikov, P. Fogla, W. Lee and W. Gong, *Anomaly detection using call stack information*, *In Proceedings of IEEE Symposium on Security and Privacy*, 2003, pp. 62-78.

[13] G. Frantzeskou, S. Gritzalis and S. MacDonell, *Source Code Authorship Analysis for Supporting the Cybercrime Investigation Process*, *1st International Conference on eBusiness and Telecommunication Networks - Security and Reliability in Information Systems and Networks Track*, Kluwer Academic Publishers, Setubal Portugal, August 2004, pp. 85-92.

[14] H. Gamboa and V.-. A. Fred., 2004., *A Behavioral Biometric System Based on Human Computer Interaction*, *In Proceedings of SPIE*, 2004.

[15] H. Gamboa and A. Fred, *An identity authentication system based on human computer interaction behaviour*, *Proc. of the 3rd Intl. Workshop on Pattern Recognition in Information Systems*, ICEIS PRESS, 2003, pp. 46 -55.

[16] A. K. Ghosh, A. Schwartzbard and M. Schatz, *Learning program behavior proles for intrusion detection*, *In Proceedings of the First USENIX Workshop on Intrusion Detection and Network Monitoring*, April 1999, pp. 51-62.

[17] T. Goldring, *User Profiling for Intrusion Detection in Windows NT*, Computing Science and Statistics, 35 (2003).

[18] A. Gray, P. Sallis and S. MacDonell, *Software Forensics: Extending Authorship Analysis Techniques to Computer Programs*, *In Proc. 3rd Biannual Conf. Int. Assoc. of Forensic Linguists (IAFL'97)*, 1997.

[19] 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)*, Springer-Verlag, Madrid, Spain, 2005, pp. 133-144.

[20] G. Gupta, C. Mazumdar and M. S. Rao, *Digital Forensic Analysis of E-mails: A trusted E-mail Protocol*, International Journal of Digital Evidance, 2 (2004).

[21] K. Ilgun, R. A. Kemmerer and P. A. Porras, *State transition analysis: A rule-based intrusion detection approach*, *Software Engineering*, 1995, pp. 181-199.

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

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

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

[25] A. R. Jansen, D. L. Dowe and G. E., *Farr Inductive Inference of Chess Player Strategy*, *Proceedings of the 6th Pacific Rim International Conference on Artificial Intelligence (PRICAI'2000)*, 2000, pp. 61-71.

[26] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, *The Design and Analysis of Graphical Passwords*, *Proceedings of the 8th USENIX Security Symposium*, Washington, D.C., August 23-36, 1999.

[27] K. Kaufman, G. Cervone and R. S. Michalski, *An Application of Symbolic Learning to Intrusion Detection: Preliminary Results From the LUS Methodology*, *Reports of the Machine Learning and Inference Laboratory, MLI 03-2, George Mason University*, Fairfax, VA, June, 2003.

[28] I. Koychev and I. Schwab, *Adaptation to Drifting User's Interests*, *In Proceedings of ECML2000 Workshop: Machine Learning in New Information Age*, Barcelona, Spain, 2000.

[29] T. Lane and C. E. Brodley, *An Application of Machine Learning to Anomaly Detection*, *20th Annual National Information Systems Security Conference*, 1997, pp. 366-380.

[30] T. Lane and C. E. Brodley, *Detecting the Abnormal: Machine Learning in Computer Security*, *Department of Electrical and Computer Engineering, Purdue University Technical Report ECE-97-1*, West Lafayette, January 1997.

[31] J. Marin, D. Ragsdale and J. Surdu, *A hybrid approach to the profile creation and intrusion detection*, *DARPA Information Survivability Conference and Exposition (DISCEX II'01)*, 2001.

[32] R. A. Maxion and T. N. Townsend, *Masquerade detection using truncated command lines*, *In International conference on dependable systems and networks(DNS-02)*, IEEE Computer Society Press, 2002.

[33] 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.

[34] M. Orozco, Y. Asfaw, A. Adler, S. Shirmohammadi and A. E. Saddik, *Automatic Identification of Participants in Haptic Systems*, *2005 IEEE Instrumentation and Measurement Technology Conference*, Ottawa, Canada, 17-19 May 2005.

[35] M. Orozco, Y. Asfaw, S. Shirmohammadi, A. Adler and A. E. Saddik, *Haptic-Based Biometrics: A Feasibility Study*, *IEEE Virtual Reality Conference*, Alexandria, Virginia, USA, March 25-29, 2006.

[36] A. G. Pennington, J. D. Strunk, J. L. Griffin, C. A. N. Soules, G. R. Goodson and G. R. Ganger, *Storage-based intrusion detection: Watching storage activity for suspicious behavior*, *Technical report CMU--CS--02--179. Carnegie Mellon University*, October 2002.

[37] Poker-edge.com, *Stats and Analysis*, Available at: http://www.poker-edge.com/stats.php, Retrieved June 7, 2006.

[38] M. Pusara and C. E. Brodley, *User re-authentication via mouse movements*, *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, ACM Press, Washington DC, USA, 2004, pp. 1--8.

[39] J. Ramon and N. Jacobs, *Opponent modeling by analysing play*, *Proceedings of the Computers and Games workshop on Agents in Computer Games*, Edmonton, Albera, Canada, 2002.

[40] K. Renaud, *Quantifying the Quality of Web Authentication Mechanisms. A Usability Perspective*, *Journal of Web Engineering, Vol. 0, No. 0*, Rinton Press, Available at: http://www.dcs.gla.ac.uk/~karen/Papers/j.pdf, 2003.

[41] M. Schonlau, W. DuMouchel, W.-H. Ju, A. F. Karr, M. Theus and Y. Vardi, *Computer Intrusion: Detecting Maquerades*, Statistical Science, 16 (2001), pp. 1-17.

[42] E. H. Spafford and S. A. Weeber., *Software Forensics: Can We Track Code to its Authors? 15th National Computer Security Conference*, Oct 1992, pp. 641-650.

[43] S. J. Stolfo, S. Hershkop, K. Wang, O. Nimeskern and C.-W. Hu, *A Behavior-based Approach to Securing Email Systems*, *Mathematical Methods, Models and Architectures for Computer Networks Security*, Springer Verlag, Sept. 2003.

[44] S. J. Stolfo, C.-W. Hu, W.-J. Li, S. Hershkop, K. Wang and O. Nimeskern, *Combining Behavior Models to Secure Email Systems*, *CU Tech Report*, Available at: www1.cs.columbia.edu/ids/publications/EMT-weijen.pdf, April 2003.

[45] M. O. Trujillo, I. Shakra and A. E. Saddik, *Haptic: the new biometrics-embedded media to recognizing and quantifying human patterns*, *MULTIMEDIA '05: Proceedings of the 13th annual ACM international conference on Multimedia*, ACM Press, Hilton, Singapore, 2005, pp. 387--390.

[46] A. Tsymbal, *The problem of concept drift: definitions and related work*, *Technical Report TCD-CS-2004-15, Computer Science Department, Trinity College*, Dublin, Ireland, 2004.

[47] C. Varenhorst, *Passdoodles; a Lightweight Authentication Method*, Available at: http://people.csail.mit.edu/emax/papers/varenhorst.pdf, July 27, 2004.

[48] O. D. Vel, A. Anderson, M. Corney and G. Mohay, *Mining Email Content for Author Identification Forensics*, *SIGMOD: Special Section on Data Mining for Intrusion Detection and Threat Analysis*, 2001.

[49] R. V. Yampolskiy, *Behavior Based Identification of Network Intruders*, *19th Annual CSE Graduate Conference (Grad-Conf2006)*, Buffalo, NY, February 24, 2006.

[50] R. V. Yampolskiy and V. Govindaraju, *Use of Behavioral Biometrics in Intrusion Detection and Online Gaming*, *Biometric Technology for Human Identification III. SPIE Defense and Security Symposium*, Orlando, Florida, 17-22 April 2006.

[51] D. Y. Yeung and Y. Ding, *Host-based intrusion detection using dynamic and static behavioral models*, *Pattern Recognition*, pp. 229-243.