STRESS DETECTION USING MULTIPLE BIO-SIGNALS

Wael Khalifa, Kenneth Revett, Mohamed I. Roushdy, Abdel-Badeeh M. Salem

Abstract: *Organizations are becoming more and more dependent on computers in their day to day activities. Employees spend hours daily interacting with various software that is needed to finish their work. This human computer interaction (HCI) may induce stress for various reasons such as bad user interface design, slow responses from the software, and much more. Stress will affect the employee's total performance and productivity, which will have a negative impact on their teams and organization. Our purpose is to have an integrated mechanism that will detect stress during HCI. The tool will be a starting point for providing a solution that aims to reduce stress in the HCI aspects at organizations. This study investigates the usage of two bio signals (EEG, ECG,) for the detection of stress during HCI.*

Keywords: *EEG Biometric, BioSignals, Stress, Multi modal, Human-computer interaction, BrainInformatics*

ACM Classification Keywords: *Experimentation*

Introduction

Computer usage has become a part of our daily routine, for entertainment and web surfing, buying products, and doing homework and of course for finishing our work. Users often get stressed in their day to day dealing with their computers. During these interactions users find many problems such as slow applications, non-intuitive user interface, lack of documentation, application freezing, etc. These incidents makes the user stressed and specially if there is some time constraint to finish the task. Another interesting scenario which may induce stress is when a person is trying to hack into a computer system. Both scenarios induce stress, but for very different reasons. This study was designed to determine if stress can in fact be reliably measured using a range of biosignals (i.e. EEG, ECG, EMG, GSR, respiration), and further, whether each stress class yields a unique signature. From the biosignals, a set of features are extracted, and instantiated with values that yield a signature for a given user. These signatures were developed by exposing the users to various types of stress inducing environments. By instantiating values for features within two stress inducing scenarios relative to control conditions, the system is able to determine on a per user basis, what type of stress they are currently feeling. Integrating this ability into the IT infrastructure may provide a mechanism that will be able to maintain stress levels within tolerable limits.

The paper is divided as follows, in section two we discuss the medical aspects of the EEG signal. Methodology is discussed in section three. Section four describes the experiment. Results are discussed in section five and conclusions are presented in section six.

Medical Aspects of EEG

The brain contains about 100 billion neurons and weighs around 1.5 KG. Neurons generate electrical signals. The sum of these electrical signals generates an electric field. Fluctuations in the electric field can be measured by devices and this is what we call Electroencephalographic (EEG) [Atwood & MacKay, 1989]. The electrical currents in the brain were discovered in 1875 by an English physician Richard Caton. He observed the EEG from the exposed brains of rabbits and monkeys. In 1924 Hans Berger, a German neurologist, used his ordinary radio equipment to amplify the brain's electrical activity measured on the human scalp [Berger, 1929]. He announced that weak electric currents generated in the brain can be recorded without opening the skull, and depicted graphically on a strip of paper. The activity that he observed changed according to the functional status of the brain, such as in sleep, anesthesia, and lack of oxygen and in certain neural diseases, such as in epilepsy [Teplan, 2002].

EEG signals are generated from activities in the neurons. When the neurons are activated, local current flows are produced [Guger et al, 2001; Coan & Allen, 2004] EEG measures mostly the currents that flow during synaptic excitations of the dendrites of many pyramidal neurons in the cerebral cortex. Differences of electrical potentials are caused by summed postsynaptic graded potentials from pyramidal cells that create electrical dipoles between soma (body of neuron) and apical dendrites (neural branches), depicted in Figure 1.

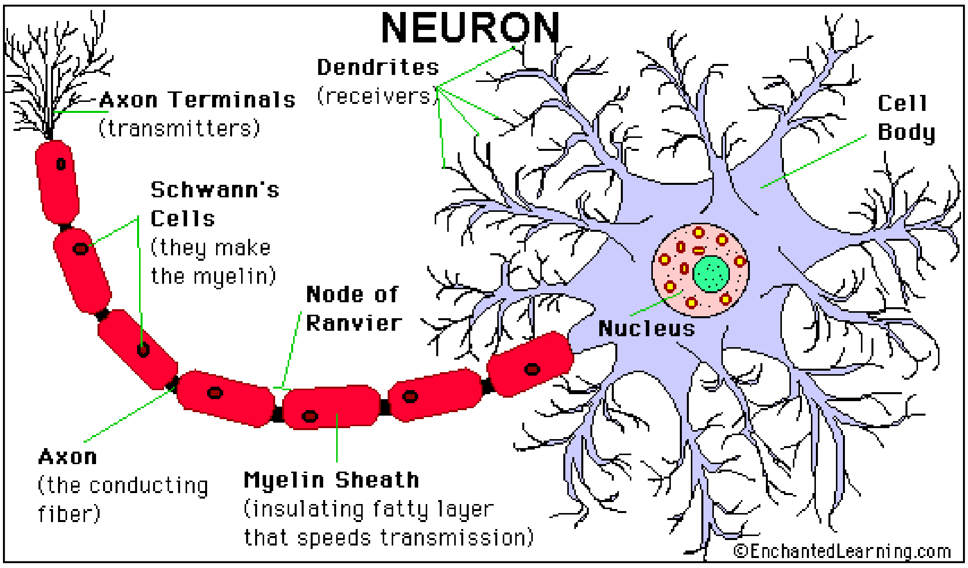


Figure 1. Basic anatomy of a typical cortical neuron, depicting the major input (dendrites), processing center (cell body), and the output region the axon [GIF, 2014]

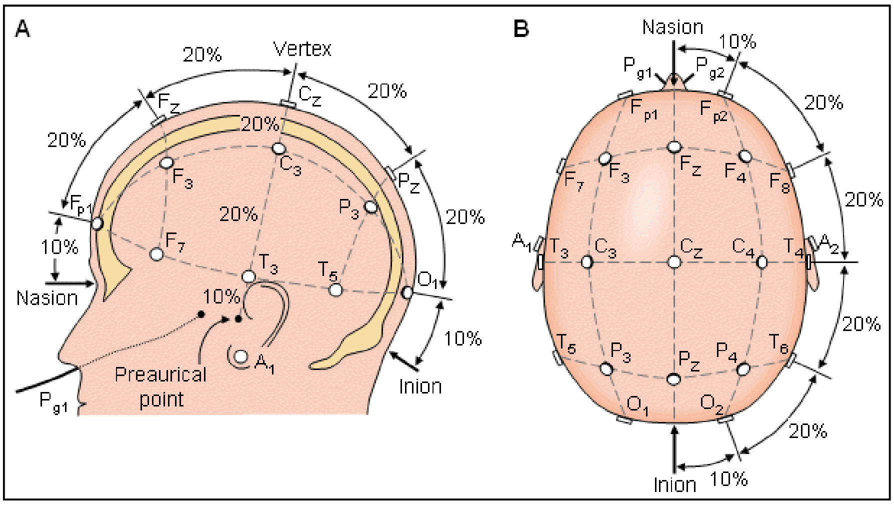


Figure 2. Electrode Placement [Malmivuo & Plonsey, 1995]

A typical EEG Signal capturing device consists of electrodes with conductive media, filters and amplifiers and analogue/digital converters. The internationally standardized 10-20 system is usually employed to record the spontaneous EEG. In this system electrodes are located on the surface of the scalp, as shown in Figure 2 A. The positions are determined as follows: Reference points are nasion, which is delves at the top of the nose, level with the eyes; and inion, which is the bony lump at the base of the skull on the midline at the back of the head. From these points, the skull perimeters are measured in the transverse and median planes. Electrode locations are determined by dividing these perimeters into 10% and 20% intervals. Three other electrodes are placed on each side equidistant from the neighboring points, as shown in Figure 2 B [Malmivuo & Plonsey, 1995].

Password Hacking Experiment

We have conducted an investigation on the neurophysiological changes that occur when a person attempts to crack a password. A password cracking scenario was provided to a small cohort of university students and while they were attempting to crack into the password, their EEG was recorded. A monetary reward was given to the fastest person to crack the password.

In this investigation, we asked volunteers (right-handed male university students, aged 20-22) to attempt to crack a password system while we acquired their EEG using the Emotiv headset [Emotiv, 2014]. The electrode positions in the 10-20 system. The subjects volunteered for this study without full knowledge of the actual purpose of the study, though they were told they would be attempting to hack into a computer system. Subjects were asked to sit in a quiet room with normal lighting. The subjects were then fitted with the Emotiv headset after assuming a comfortable position in an armchair placed in front of a laptop computer. Further, we deployed both ECG (3-lead) and a blood pulse volume electrode (placed on the left ear lobe) in order to acquire information regarding heart rate variability. We used the Vilistus system for the ECG and BVP recordings [Vilistus, 2014]. Moreover, the keystroke data was recorded for key stroke analysis.

The experiment started once all of the electrodes (EEG, ECG, and BVP) were positioned and the recording signal was stable. The subjects were asked to relax as much as possible all subjects indicated that the recording equipment was not uncomfortable and did not obstruct their hand motion during typing in any way. The experiment protocol used in this study is depicted in Table 1. Note all phases of this experiment were carried out using a standard 102-keyboard integrated into a laptop. All subjects were filmed during the experiment and all software deployed (the Emotiv TestBench and the Vilistus (v 1.2.38 professional)) and video recording were synchronized to a common clock for subsequent data processing and analysis.

Table 1. Experiment Stages

Task	Duration	Purpose
Reading	1-5 Min	Act as a baseline
Transcriptional Writing	1-5 Min	To discover the Biosignal pattern of writing
Login	-	Baseline for key strokes
Reading	1-5 Min	Return user to baseline
Password Hacking	Max 5 Min	The experiment
Authenticate	-	Baseline for key strokes

Stage 1: Reading a page of text, the user was asked to read a peace of text about body language, the user cannot move to the next stage until at least one minute elapses. The user can stay at most five minutes at this stage. If the user finished reading the article before the five, they can press next for the next stage of the experiment. If the five minutes elapses the user is advanced automatically for the next stage.

Stage 2: The subjects were asked to type in a page of text containing approximately 300 words. This text contained the same text the user read at stage 1. Again the same 1 minute and 5 minute rule described in stage 1 applies here. The screen is divided to two sections the above section show the text and below section for writing. On the top left corner two counters are shown for the user. The word per minute count, which is the user typing speed and the number of errors done. The error is typing text different than the text body. Users are encouraged to type as fast as possible while maintain low error count.

Stage 3: User login, the user is asked to login using his university username and password. This data is used as a baseline for keystroke dynamics.

S**tage 4**: Upon completion of this task, the subjects were asked to read another page of text (which was different from the original page they read) silently. The text is very generic information about how to hack into computer systems, extracted from a website. The behavior and look of stage 4 is exactly like Stage 1.

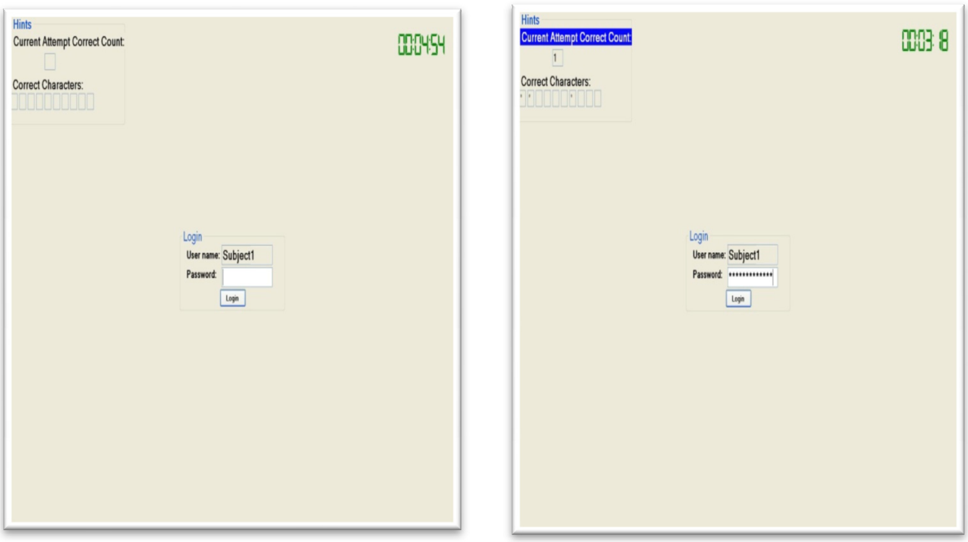
Stage 5: Once this task was completed, the subjects were then provided with the account hacking scenario. This scenario attempted to reproduce the hacking process as much as possible.

- Before the experiment start the user was presented with the legitimate user profile which includes his name, date of birth, phone number, hobbies and interests;
- The user was told that the password is a combination of the above data;
- The subjects were told that they had to try to hack a 10 character password in 5 minutes;
- Note the hints were presented before the experiment began and were not displayed during the hacking scenario;
- As the subject correctly 'hacked' elements of the password (which were all lower case letters and digits), they were displayed as asterisks '*' in there correct position (see Figure 5 for details) on the screen;
- A timer was positioned on the screen in the upper right hand corner of the screen (in the default color green);
- After the 2-minute mark, the timer digits color was changed to RED;
- The presentation of the time was meant to induce stress in the subjects during the hacking process;
- At the end of the 2-minute mark, 50% of the characters correctly 'hacked' were displayed (half + 1 if the number of hacked entries was odd);
- At the end of the next minute, 50% of the remaining correctly hacked characters were revealed, and at the last minute, all characters were displayed in addition to any newly discovered elements until the test terminated;
- This test phase of the experiment terminated when either the password has been cracked or the timer has expired.

Figure 3 shows sample of the password hacking screens.

Stage 6: the user is asked to login using the hacked username and password. If time elapsed and the user failed to hack the password the password is shown briefly and the user is asked to use them for login.

Stage 7: The subjects were then de-briefed and thanked for their participation.



User name: Subject1
Password:

User name: Subject1
Password: *************

Figure 3. The left hand panel presents the hacking scenario form 6 seconds into the start of the hacking scenario. The right hand panel presents the same subject 81 seconds later, with 2 correctly guessed characters of the password

Between each stage a screen is shown for three seconds that tells the user what’s the next stage and gives a user a break between tasks

Data Analysis and Results

Once the test was completed, the data was saved and analyzed off-line using EEGLab (v 9.0.4.6) for the Emotiv EEG data and Matlab (v7.0.6.324, R2008a) scripts were used for analyzing the heart rate variability data acquired from the ECG and BVP electrodes [Emotiv, 2014; EEGLAB, 2014]. The EEG data was obtained using the emotive headset, which contains 14 dry electrodes and 2 mastoid reference electrodes. The electrode positions and 10-20 system labels are depicted in Figure 4. In order to reduce motion artefacts, subjects were requested to sit as still as possible, with elbows placed firmly on the arms of the chair. The EEG was recorded and event markers were generated whenever excessive subject movement was noted. A digital recording of the experiment was also acquired to provide additional criteria for motion artefact detection to enhance the quality of the data. In addition, the BVP and ECG were utilized to assist in motion artefact, detection, and the video recording assisted in eye blink detection and synchronization as well.

Briefly, the EEG data was collected at 128 Hz with mastoid referencing in EDF (European Data Format) format, which can be directly imported into EEGLab (which runs within Matlab). A channel location file was generated which corresponded to the electrode layout for the Emotiv headset, and care was taken to ensure that the electrodes were positioned at the same positions across all subjects.

The first processing stage requires that markers are placed in the data indicating the start, termination point, and the phase boundaries. All recording components were synchronised to a digital clock and audio data was also deployed in order to indicate boundary points. Eyeblinks can be an effective means of placing timer marks in the data – they can be caught on camera as well and serve as useful and frequent time event markers. Timing (event markers) were placed in the datasets (note all recoding modalities were acquired at the same sampling rate of 128 Hz) for subsequent analysis. In the next phase, data cleansing was required in the form of artefact removal. The data was first examined for gross artefact detection manually – any sections of the recording that contained significant artefacts were rejected. All rejected segments were removed from the data and the 'cleansed' data was utilized for further processing.

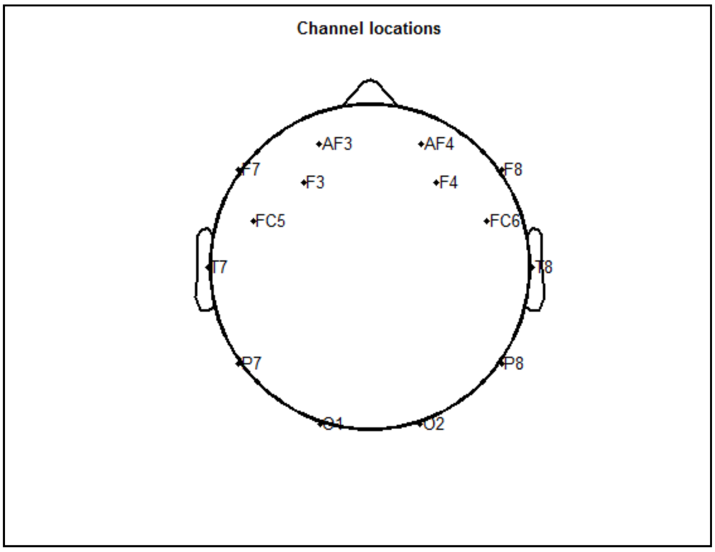


Figure 4. A screenshot of the Emotiv headset electrode position and labeling scheme deployed in this study

The heart rate variability (HRV) was also deployed in order to provide additional information about typing and the 'hacker' tasks. Data for HRV analysis was acquired using both 3-lead electrocardiogram (ECG) and blood volume pulse (BVP) monitoring was performed using a photoplethysmograph (PPG) placed on the left earlobe. All data acquired form HRV determination was band passed filtered (1-50 Hz) prior to further processing.

The data was epoched according to experimental phase in the same fashion as the EEG data, and artefact removal and band pass filtering (0.1-40 Hz) was performed. Any missing elements were filled in with baseline values to maintain temporal correlation with the EEG dataset. The BVP serves as a separate measure of heart rate which recorded the changes in the volume of the underlying vasculature when the heart beats. It is generally considered less susceptible to noise then the ECG and tends to produce more stable data then the ECG. The level of physiological data that can be extracted using BVP is more limited then the ECG in general, as it does not provide cardiac physiology details. It was deployed in this study to determine how well it correlated with the ECG in terms of capturing HRV data. The key advantage to BVP is the simple method used to obtain the data – a simple clip on the ear lobe is typically deployed and could be integrated into a headphone that are currently employed in many mobile phones and portable listening devices.

The EEG analysis focused on a subtraction method, whereby data from phase II – the typing phases was analysed with respect to phase I – the reading phase. Any differences in the recordings between these 2 phases would represent the difference between the tasks – namely the EEG correlates of typing. Likewise, the hacking phase (phase V) data was subtracted from the subtracted phase II data – the typing phase, in order to reveal changes associated with the hacking component. Since this is a preliminary study, aimed at producing an appropriate design methodology, not all possible outcomes were examined. The results from this analysis are presented in the next section.

The HRV was measured using a method which determines the distance between the peaks of each heart beat. The peak of the QRS wave is sought for all heart beats, and the time between peaks is measured (variation in beat-to-beat interval). Variations in beat-to-beat intervals is recorded and used to access the physiological stress the subject may be experiencing [Palaniappan & Krishnan, 2004; Revett et al, 2010]. The experiment of induced hacking was designed to simulate the expected stress levels associated with a time based task and it is reasonable therefore to assume that the subject will experience stress. The deployment of ECG and BVP was designed to determine whether or not this assumption held in our experimental paradigm.

Results

The principal result obtained from this experiment was that the subject did feel that they were under physical stress during the hacking scenario. This result is predicated on changes in HRV which was recorded throughout the experiment. The results in Table 2 depict the average HRV within each of the four phases of the experiment across all three subjects.

Table 2 Heart rate variability presented as the average across all subjects for each experimental phase. HRV was measures as the coefficient of variation (CV) for the last 100 heart beats in each phase.

Table 2. HRV Rate VS Stages

Stage	Reading 1	Writing	Reading 2	Hacking
HRV	0.3%	1.1%	0.5%	3.8%

The HRV was significantly larger ($p < 0.001$) for the phase IV subjects, and this held true across all subjects. The same trend held for the BVP measurements, which indicates a variation on the heart rate of the subject. Further, the subjects self reported that they felt under stress when trying to hack the password.

Further confirmation was obtained by analyzing the video recording of the subjects, which captured the subjects' actions throughout the experiment. All subjects appeared agitated, displaying a variety of facial grimaces and general heightened arousal during the hacking phase relative to the reading and typing phases.

The EEG results indicated significant changes in the power spectrum during various stages of the experiment, which varied across electrodes. The difference between the transcriptional typing and reading phases suggested that the F3 electrode and both occipital electrodes (O1 and O2) especially displayed a high level of activation during transcriptional typing relative to reading alone. The alpha frequency band (8-12 Hz) power was raised significantly relative to the reading alone scenario, with other bands appearing roughly equal in power. The second reading task was not significantly different from the initial reading task (Phase III v Phase I), though there was a non-significant change in the delta band (1-4 Hz) power spectrum in the occipital field electrodes (O1 and O2). The hacking scenario produced the most significant changes of all phases.

The power spectrum for the more frontally position electrodes (F3 and AF3) were strongly elevated relative to the transcriptional typing phase of the experiment in the alpha band. In addition, there was reduced activation of the occipital electrodes (O1 and O2) relative to the transcriptional typing task (across all frequency bands). Thus a pattern emerged which was consistent across all subjects: hacking yielded a reduced occipital power spectrum across all frequency bands, and yielded elevated activity pattern in the frontal electrodes (F3 and AF3) in the alpha band relative to transcriptional typing and reading.

Table 3 summarizes the changes in spectral power across all major frequency bands for each of the experimental phases. The results are the grand averages across all subjects. These results are for the frontal electrode (F3 and AF3). Note that there are also changes in the occipital electrodes (O1 and O2), as indicated in the text. Note the reading task was assumed to be the control for this experiment.

Table 3. EEG Analysis

Stage 1	Stage 2	Phase 4	Phase 5
Delta - 1.0	Delta - 1.1	Delta - 1.0	Delta - 1.3
Theta – 1.0	Theta – 1.2	Theta - 1.2	Theta - 1.5
Alpha – 1.0	Alpha – 2.6	Alpha - 1.2	Alpha – 4.2
Beta – 1.0	Beta – 1.4	Beta - 1.1	Beta - 1.2

Conclusion

This study had two principal objectives in mind: 1) to record the EEG from subjects while engaged in typing and 2) to determine how the EEG changes when a person is attempting to hack into a computer system by password guessing. The experimental paradigm was designed to incorporate controls for both pure transcriptional typing and the password hacking task. The transcriptional typing component entailed a dictation protocol, where the subjects were asked to type what they were reading in real time. Further, the typing of text was used as a control for the hacking component, which also involves typing. Typing is a very common motor task that involves a series of steps: reading the text, hand positioning, and the actual typing movements. Which parts of the brain are engaged during this task has not been clearly presented in the literature to date (though see [Reiera et al, 2008; Palaniappan & Revett]).

The results presented in this study indicate that there are particular regions of the brain that become activated during transcriptional typing (see [Jönsson, 2007]). The EEG headset contained 14 electrodes (excluding two mastoid references), as such it could certainly be the case that other regions of the brain could yield additional changes that were not recorded in this experiment because of a small electrode set. This can be examined by using a much larger electrode array (we are planning to use a high resolution 128 BioSemi system in the near future to examine this issue in detail).

The actual hacking scenario did produce a change in the overall power spectrum that was reproducible across all subjects. The pattern was based on relative changes in power across frequency bands, a common measure that reflects the brain activity within a given frequency band. The pattern that emerged in this study was that transcriptional typing produces a unique pattern relative to a passive reading task. This is a novel result and will be explored more fully using a quantitative EEG electrode setup. Furthermore, this study produced results indicating that the actual process of password hacking yields a characteristic signature when examined using EEG, ECG, and PPG. The ECG and PPG results provide information on the stress level of the individual – the heart rate variability is a significant indicator of stress level – and PPG is typically deployed to record physical exertion level – though it is suggested by this study that it can also be used to measure mental exertion as well. The two measures provided physiological evidence that password hacking per se can induce a mental exertion which causes changes in HRV and heart rate generally [EEGLAB, 2014; Palaniappan & Krishnan, 2004; Revett et al, 2010], The EEG data suggests that there is a unique brain activation pattern associated with password hacking that can be recorded using a small electrode helmet such as that available in the Emotiv headset. These results suggest that a profile of a hacker can be deduced readily – based on the physiological responses engendered by the hacking process. Whether these results would hold true for a 'professional' hacker is a point that requires further investigation. The subjects deployed in this study were Nubian hackers and these results may simply reflect their lack of expertise in this task.

What needs to be considered in this work is that whether the experiment had sufficient controls. In the next phase of this work, a more stringent phase II will be produced, where the subject will be asked to reproduce the text corpus in a fixed time period without error. In this study, the subjects were able to complete the transcriptional typing without undue stress. This was by design, as we wished to determine the effects of typing alone. It would be interesting to compare two tasks that involve typing – both eliciting a stress reaction from the subjects, whereby one of the tasks involved hacking. This approach may eliminate stress per se – the stress of task completion from the act of hacking. Clearly, we do not wish subjects whom are under stress to be considered hackers! But if we measure stress – this should result in a general alert being raised. If the stress is associated with access entry activity – then a higher level of alert should be raised. The system indicated in this paper could be implemented autonomously and could then be used to decide whether the stress is due to the intention of the user – to hack into the system – or simply reflects and overworked and under paid employee.

Acknowledgement

The paper is published with partial support by the project ITHEA XXI of the ITHEA ISS (www.ithea.org) and the ADUIS (www.aduis.com.ua). We thanks them both for the opportunity and support for publishing this paper

Bibliography

[Atwood & MacKay, 1989] H. L. Atwood, W. A. MacKay., "Essentials of neurophysiology," B.C. Decker, Hamilton, Canada, 1989.

[Berger, 1929] Berger, H., Ueber das Elektroenkephalogramm des Menschen, Archiv für Psychiatrie und Nervenkrankheiten, 1929, Berlin, 87: 527-570.

[Coan & Allen, 2004] Coan, J.A. & Allen, J.J.B., (2004) Frontal EEG asymmetry as a moderator and mediator of emotion, Biological Psychology, 67, pp. 7-49.

[EEGLAB, 2014] EEGLAB: http://sccn.ucsd.edu/eeglab/ (26/4/2014)

[Emotiv, 2014] Emotiv: http://www.emotiv.com/ (26/4/2014)

[GIF, 2014] GIF: http://www.enchantedlearning.com/subjects/anatomy/brain/gifs/Neuron (26/4/2014)

[Guger et al, 2001] Guger C., Schlög A., Neuper C., Walterspacher D., Strein T., Pfurtscheller G., “Rapid Prototyping of an EEG-Based Brain-Computer Interface (BCI)”, IEEE Transactions on Neural Systems and Rehabilitation Engineering, Vol.9, No. 1, March 2001

[Jönsson, 2007] Jönsson, P., (2007) Respiratory sinus arrhythmia as a function of state anxiety in healthy individuals, International Journal of Psychophysiology 63: 48–54.

[Malmivuo & Plonsey, 1995] Jaakko Malmivuo and Robert Plonsey, Bioelectromagnetism Principles and Applications of Bioelectric and Biomagnetic Fields, Oxford University press, 1995

[Palaniappan & Krishnan, 2004] Palaniappan, R. & Krishnan, S.M., (2004) Identifying individuals using ECG beats, in proceedings of the International Conference on Signal Processing and Communications (SPCOM ’04), pp. 569-572, Bangalore, India.

[Palaniappan & Revett] Palaniappan, R. & Revett, K., Thought Based PIN Generation Using Single Channel EEG Biometric, International Journal of Cognitive Biometrics, in press.

[Reiera et al, 2008] Riera, A., Soria-Frisch, A., Caparrini, M,. Grau, C. & Rufini, G., (2008), Unobtrusive Biometric based on electroencephalogram analysis, EURASIP Journal on Advances in Signal Processing, pp.1-8.

[Revett et al, 2010] Revett, K., Deravi, F., & Sirlantzis, K., (2010) Biosignals for User Authentication - Towards Cognitive Biometrics?, EST’2010, International Conference on Emerging Security Technologies, University of Kent, Canterbury, 6-8 September, 2010, pp.71-76,

[Teplan, 2002] Teplan, M, “Fundamentals of EEG Measurement,” in Measurement Science Review, vol. 2, pp. 1–11, 2002.

[Vilistus, 2014] Vilistus: http://www.vilistus.com/products.shtml (26/4/2014)

Authors' Information

Wael Khalifa - *Ph.D. student at faculty of computer and information sciences, Ain Shams University, e-mail: wael.khalifa@cis.asu.edu.eg*

Kenneth Revett – *professor of Computer Science at Computer Science Department, British University in Egypt*

Mohamed I Roushdy – *Dean of faculty of computer and Information sciences, Ain Shams University, Abbasia, Cairo-Egypt; e-mail: miroushdy@hotmail.com*

Abdel-Badeeh M. Salem - *Professor of Computer Science*
Head of Artificial Intelligence and Knowledge Engineering Research Labs,
Faculty of Computer and Information sciences,Ain Shams University, Cairo,Egypt
e-mail: abmsalem@yahoo.com