# In the Hacker's Eye: The Neurophysiology of a Computer Hacker

Wael Khalifa[1], Kenneth Revett[2], and Abdel-Badeeh Salem[1]

[1] Faculty of Computer and Information Science
Ain Shams University
Abbassia
Cairo, Egypt
{wael.khalifa,absalem}@asunet.shams.edu.eg
[2] Faculty of Informatics and Computer Science
British University in Egypt
El Sherouk City
Egypt
ken.revett@bue.edu.eg

**Abstract.** This paper presents data from a preliminary 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. The results indicate that the overall frontal lobe power (at electrode position F7) was significantly different during cracking as opposed to typing alone. Further, the principal visual area (O1 and O2 electrodes) electrodes displayed much more variability in the cracking scenario than in the transcriptional typing scenario. Further, the anterior frontal electrodes displayed much higher activation than in the transcriptional typing task. These results suggest that using EEG recording alone, a unique signature can be acquired in real-time which provides significant and suggestive evidence that the user is not merely typing – that they may be trying to crack into the system.

**Keywords:** affective computing, biometrics, electroencephalography, heart rate variability, neurophysiological computing, password hacking.

## 1 Introduction

This pilot study had two principal aims: 1) to investigate the effect of typing on the EEG and 2) to investigate whether a person attempting to hack into a computer system by on-line password cracking could be identified using standard electroencephalography (EEG) technology. The password cracking scenario was implemented using subjects that manually (as opposed to an automated character generating approach) attempted to guess a user's password while sitting at the host machine. This approach requires the user to type entries and as such, there are two elements involved in this process that are relevant here: i) the actual typing process and ii) and the hacking process. The assumption utilised in this study is that is that by

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 112–119, 2012.

subtracting out the typing element during keyboard entry based password cracking, we would be left with the 'cracking' aspects of this behavior. It is interesting to note that the literature is sparse on the effects of typing on the EEG – i.e. that those aspects of cognition involved in typing have not yet been elucidated based on published literature. A side effect of this paper is to provide some basic data on brain activation patterns that occur during transcriptional typing. Subjects are asked to perform keyboard entry of a small corpus of text (approximately 300 words) prior to the hacking scenario. The subjects were asked to type the corpus with no time limit – which was completed in approximately 10 minutes (range 7 +/- 2 minutes). The subjects were told that they did not have to worry about correctness – though the typing errors were on the order of 10%, indicating that the subjects were consciously attempting to correctly enter the corpus text.

Transcriptional typing also entails reading the text while typing, typically using an interleaving approach where text is read and stored in a 'mental buffer' – short term memory and the typed. Professional typists will be able to type without looking – and hence they can read the text continuously while typing, thereby producing very fast typing rates (60+ wpm). The subjects were university students and hence not professionally trained typist. They deployed a 'read-store-type' loop during the typing process and produced typing speeds of approximately 30 wpm. The critical issue with respect to the transcriptional typing task is to control for the reading sub-task which is implicit in transcriptional typing. We asked subjects to read a small corpus of text prior to typing corpus of the same length (but different) text. The goal here is to try to identify those activation patterns associated with reading and subtract these patterns from the transcriptional task. In theory, this would leave only those activities associated with typing, which in turn would be removed from the hacking scenario, yielding activity patterns associated with hacking per se.

## 2 Methods

It is for obvious reasons difficult to acquire physiological recordings while a person is attempting to hack into a computer system. 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 system. The subjects volunteered (three in this pilot) 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 [1],

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. The experiment consisted of four contiguous phases as 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 Evotiv 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.** Experimental protocol used in this study. Note that the text corpus read in stages 1 and 3 was the same, and different from the corpus deployed in the transcriptional typing task.

| **Read silently** (2 minutes) | **Transcriptional Typing** (10 minutes) | **Reading silently** (2 minutes) | **Login test** (0.5 minutes) | **Hacking** (5 minutes) |
|---|---|---|---|---|

After reading the page of text (stage I), the subjects were asked to type in a page of text containing approximately 300 words. This text contained very generic information about how to hack into computer systems, extracted from a website. 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 (stage III). 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. 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 on the screen. At the end of the 1st minute, a timer was positioned on the screen in the upper right hand corner of the screen (in the default color black). After the 2-minute mark, the timer digits color was changed to RED and the size of the image box which contained the numerical digits of the time in a standard stopwatch timer countdown format was enlarged so it was more conspicuous. 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. The subjects were then de-briefed and thanked for their participation.

Once the test was completed, the data was saved and analysed 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 [2,3]. The EEG data was obtained using the emotive headset, which contains 14 dry electrodes and 2 mastoid reference electrodes (adhering to the 10-20 electrode system). 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 subjects were asked to type on a standard laptop style 102-keyboard which was positioned at a

level and distance deemed to be comfortable for each subject. 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 utilised 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 utilised for further processing.

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 IV) 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 [4,5]. 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.

## 3 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.

| Phase I | Phase II | Phase III | Phase IV |
|---|---|---|---|
| 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.** Summary of 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.

| Phase I | Phase II | Phase III | Phase IV |
|---|---|---|---|
| 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 |

## 4 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 [6,7]). The first stage of this study was designed to acquire quantitative data to determine which part(s) of the brain is/are correlated with typing as determined from EEG recordings. The results presented in this study indicate that there are particular regions of the brain that become activated during transcriptional typing (see [8]). 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).

## 5 Discussion

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 [9,10,11]. 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!

**Acknowledgement.** We would like to thank the students from the British University in Egypt, Faculty of Informatics and Computer Science for their kind participation.

## References

1. Vilistus: http://www.vilistus.com/products.shtml
2. EEGLAB: http://sccn.ucsd.edu/eeglab/
3. Emotiv: http://www.emotiv.com/
4. Palaniappan, R., Krishnan, S.M.: Identifying individuals using ECG beats. In: Proceedings of the International Conference on Signal Processing and Communications (SPCOM 2004), Bangalore, India, pp. 569–572 (2004)
5. Revett, K., Deravi, F., Sirlantzis, K.: Biosignals for User Authentication - Towards Cognitive Biometrics? In: EST 2010, International Conference on Emerging Security Technologies, University of Kent, Canterbury, September 6-8, pp. 71–76 (2010)
6. Coan, J.A., Allen, J.J.B.: Frontal EEG asymmetry as a moderator and mediator of emotion. Biological Psychology 67, 7–49 (2004)
7. Riera, A., Soria-Frisch, A., Caparrini, M., Grau, C., Rufini, G.: Unobtrusive Biometric based on electroencephalogram analysis. EURASIP Journal on Advances in Signal Processing, 1–8 (2008)

8. Palaniappan, R., Revett, K.: Thought Based PIN Generation Using Single Channel EEG Biometric. International Journal of Cognitive Biometrics (in press)
9. Jönsson, P.: Respiratory sinus arrhythmia as a function of state anxiety in healthy individuals. International Journal of Psychophysiology 63, 48–54 (2007)
10. Luay, M., Revett, K.: On the applicability of heart rate for affective gaming. In: WSEAS Special Session on Knowledge Engineering for Decision Support Systems, the CSCC Multiconference, Corfu Island, Greece, July 15-17, pp. 267–272 (2011)
11. Cacioppo, J.T., Bernston, G.G., Larsen, J.T., Poehlmann, K.M., Ito, T.A.: The psychophysiology of emotion. In: Lewis, M., Haviland-Jones, J.M. (eds.) Handbook of Emotions, 2nd edn., pp. 173–191. The Guilford Press, New York (2004)