GRAND ACADEMIC PORTAL
RESEARCH JOURNALS

GAP iNTERDISCIPLINARITIES
A Global Journal of Interdisciplinary Studies
(ISSN – 2581-5628)
Impact Factor: SJIF - 5.047, IIFS - 4.875

GRAND ACADEMIC PORTAL (GAP) 2017
ज्ञान: अध्ययन: परम्परा

CYBER CRIME INVESTIGATION THROGH BEOS PROFILING

Grandhi Saroja Roy, Dr. Priyanka Kacker

M.Sc. Forensic Psychology, Institute of Behavioural Sciences,
Gujarat Forensic Sciences University, Gandhinagar, Gujarat
sarojaroy@grandhi@gmail.com

Assistant Professor, Institute of Behavioural Sciences,
Gujarat Forensic Sciences University, Gandhinagar, Gujarat
drpriyankakacker@gmail.com

Abstract

Due to issues of proximity and remoteness, the identification of cyber-crime offending will often rely on circumstantial evidence and electronic information obtained during Digital Forensic Investigations. This arises difficulty in attributing ownership and authorship to electronically stored information, and also in identifying individuals in control of information systems and devices. The purpose of this study is to find out if BEOS can help in finding the offender by using the actions and techniques applied in Hacking for designing the probes. Brain Electrical Oscillations Profiling (BEOS) profiling is a technique primarily developed as a forensic tool for deception detection in suspects which was developed and tested by Dr. C. R. Mukundan. Analyzing the electrophysiological data recorded from scalp of a subject, the test is expected to provide information on the presence of "Experiential Knowledge" of participation in any act. Subjects were selected through purposive method of sampling where five Professional hackers and five Amateur hackers were involved in this study. Two sets of probes were designed for the BEOS profiling, one using the Specific experience narrated by the participant, and other being Standard set for all referring to most commonly performed Social engineering hacking method i.e., Phishing. BEOS profiling was conducted and the reports were analyzed. The comparison of Experiential Knowledge elicited between the Specific and Standard sets has shown no significant difference, allowing us to state that we can use Standard process of attack or breach identified, for designing the probes to conduct BEOS profiling of the suspects, when no electronic evidence is collected or available to determine specific traces. Overall, the results showed positivity for the use of BEOS profiling in cyber-crime investigations, when there is difficulty in identifying the suspects and the attribution of their ownership to the electronic evidence collected is in doubt.

Keywords: Cyber-crime, Digital Forensic Investigation, Hacking, Brain Electrical Oscillations Profiling, Experiential Knowledge.

INTRODUCTION

Technology has become the means, subject, tool, focus, and object of crime. Although technology eases the commission of traditional crimes, like offenses causing personal harm and offenses against property [1], current national legal frameworks may be incapable of addressing rapidly evolving 'modus operandi' associated to cyber-crime offending [2]. Cyber-crime can be committed inexpensively and easily, and victims aren't able figure out if offender is "half a block or half a world away. The anonymity of cybercrime also increases the magnitude of offending and obstructs efforts to identify culprits, thereby distinguishing it from physical crimes [3]. The disinhibiting effect of technology serves to psychologically distance the criminals from the consequences of their victimizing behavior [4]. In addition to advanced technical aptitudes, cyber criminals have skills in linguistics and psychology, which they combine to execute social engineering deceptions, manipulate decision-making processes, and distort perceptions [5].

Hacking in simple words is an attempt to exploit any computer system or a private network inside a computer. It is defined as the process of accessing computer systems by persons who have no legitimate access to the systems[6]. In general hacking is associated with breaking the law and it is assumed that everyone who engages in hacking related activities is a criminal. Granted, there are individuals who use hacking techniques to break or bend the law, but hacking isn't always about that. In fact, hacking has more to do about following the law than breaking it.

Prof C.R. Mukundan developed a forensic investigative tool. BEOS (Brain Electrical Oscillations Signature) Profile. It is a computer-based technology to identify the presence of "ExperientialKnowledge" in the perpetrator of the crime. This technique is used for extracting a signature of electrical oscillations from thebackground electrical activity of the brain of a subject by presenting a probe. The signature contains

https://www.gapinterdisciplinarities.org/

reference to an "Experiential Knowledge" (EK) in the subject to an act committed by the person, and which is elicited by the probe using the method of Probing. The probe makes the subject become awareof the experience or the action, if he or she has committed the same. During recall of the EK the subject recalls the autobiographical information related to the occurrence of the event and subject's participation in the act [7].

The primal difference between the perpetrator of a crime and an innocent personis that the perpetrator, having committed the crime, has the details of the crime stored in hismemory as signatures, and the innocent suspect does not. This is what Brain fingerprintingtesting detects scientifically, the presence or absence of specific information [8].

It can be very problematic to establish a relation between electronic evidence and an offender [9]. Typically, a mix of direct and circumstantial evidence must be assembled to place a suspect 'behind a device' at a particular time and place [10]. Electronic evidence is usually supplemented by evidence obtained through traditional police investigations to demonstrate that a particular device was under the control of a suspect when the offending occurred. In cases where the defendant is charged with possession of illegal material, the prosecution will need to establish that the defendant had knowledge of, and therefore intended to possess, the material. Electronic evidence is often transient and rarely exists in isolation. It is a product of the computer program used to generate the information and the computer system, which directed the activity [11]. The question of authorship is regularly raised in cyber-crime investigations, from theft of intellectual property to money laundering, as well as many types of fraud. This study focuses on minimising this issue of question of authorship using probing through BEOS and exploring its efficiency in cybercrime investigations.

RATIONALE OF THE STUDY

The focus of the present study is to explore whether eliciting experiential knowledge on hacking process is possible using probe presentation in BEOS. In hackers, to provoke or trigger their remembrance on hacking experiences, the probes must be designed in such a way that they are clearly referring to the cyberspace and virtual components they are working on. In forensic investigations, the process starts from finding the evidences, analyzing the modus-operandi, criminal profiling and identifying the suspect. Many cases were investigated by probe presentation in BEOS using the modus operandi, statements given by the people involved in the incident (witnesses, victims and suspects) and the investigating officer. Similarly, even in investigating cybercrimes, the traces left while exploiting are identified, electronic information is collected and the process is analyzed. As they are no record of studies till now which stated that probe presentation in BEOS can elicit experiential knowledge in hacking process, this study aims towards the use and efficiency of Brain Electrical Oscillations Profiling (BEOS) in cybercrime investigations and in identifying the suspect involved in cyber breaches or attacks.

OBJECTIVE

The aim of this research is to study whether Experiential Knowledge can be generated on Hacking process in an individual involved in hacking using Auditory Probe Presentation in BEOS.

HYPOTHESIS

1. Experiential knowledge can be elicited on Hacking process using Probe presentation in BEOS.
2. H_0 - There will be no difference in EK elicited between Specific Hacking and Standard Hackingamong all the subjects.
3. H_0 - There will be no difference in EK elicited between Specific Hacking and Standard Hackingamong the Professional Hackers.
4. H_0 - There will be no difference in EK elicited between Specific Hacking and Standard Hacking among the Amateur Hackers.

METHODOLOGY

Participants

Subjects for the study were selected through Purposive Sampling technique from Gandhinagar, Gujarat. Age group was 20-25 years. Total sample size is 10, divided into two groups with 5 subjects in each group. One group is of Professional hackers and the other group consisted of Amateur hackers. Informed consent was taken from each subject.

Tools and Instruments Used

Brain Electrical Oscillations Signature (BEOS) Profiling

BEOS Profiling was conducted in the study. BEOS profiling is a technique primarily developed as a forensic tool for deception detection in suspects which was developed and tested by Dr. C. R. Mukundan. Analysing the electrophysiological data recorded from scalp of a subject, the test is expected to provide information on the presence of "experiential knowledge" of participation in any act. The scientific basis of the test uses the distinction between recognition using familiarity or knowledge and remembrance of experience from autobiographical memory of the individual.

The BEOS consists of two major systems, Neuro Signature System (NSS) for the acquisition of brain electrical activity and Visual and Auditory Stimulus Programming (VASP) system for the purpose of recording the auditory and visual probes and their presentation while interacting with data acquisition system.

Procedure

In order to fulfil the objective of the study, a proper format is decided upon. The format was to collect a narration of specific hacking experience of the subject to make one set of probes and to select a standard common hacking process to design standard set of probes to be presented and tested on the subjects.

The participants were asked to write one specific hacking episode they have done in detail. I chose Phishing, the most common social engineering attack in hacking, to create standard set of probes. The standard set consisted of 68 probes divided into 8 scenarios including Control and Neutral Probes. The Specific sets consisted of 56 minimum and 79 maximum probes divided into 6 to 11 scenarios including Neutral and Control probes. Event Markers were given to each respective probe. The sets were uploaded into VASP after which the auditory probes were recorded, based on the gender. The recorded probes are then saved and uploaded into recorded probes in the VASP, which will automatically upload them into NSS for presentation during the BEOS testing.

The subjects were called to the BEOS lab for recording. Prior to the testing, it was ensured that the temperature of the room was not hot and it was also ensured that the subject has removed his/her watches or any other metal things. The subject was asked to keep away any electronic devices as it may hamper the recording. The subject was seated comfortably in a wooden chair. The subject was asked to rest their arms on the arm rest. The harness was worn around the subject's chest. Then the head cap with 32 channels was placed on the subject's head. The placement of the head cap was significant for proper recording. The saline gel was then infused into electrodes using a syringe with the blunt needle. The reference point is attached to the earlobe and using the connector the head cap is then connected to the amplifier. The subject is asked to close the eyes for a baseline recording which lasts for 2 minutes. After the baseline session, a BEOS session is conducted where the probes are presented. The subject is asked to close the eyes and then the probes will be presented to the subject. Each probe is presented and there is a gap of 6 seconds between the presentations of probes. The gap is because the brain requires 6 seconds to respond to each probe. And it was also instructed that subject should not sleep while recording, otherwise the probe presentation will be stopped automatically. The data generated by BEOS after testing was evaluated for further analysis and results.

RESULTS AND DISCUSSION

Due to issues of proximity and remoteness, the identification of cybercrime offending will often rely on circumstantial evidence and electronic information discovered during Digital Forensic Investigations to establish that a particular suspect was in control of a device when an offence occurred. This arises difficulty in attributing ownership and authorship to electronically stored information, and also in identifying individuals in control of information systems and devices [12]. Through this study, we tried to find out up to how far BEOS can help in pointing out the offender by using the actions and techniques applied in attack, traced by analysing electronic information and evidence obtained in investigation, for designing the probes.

Table 1. No. of Probes eliciting EK and Percentage of EK elicited in Specific set of Probes

Participants	Specific	Total No. Of Specific Probes	Percentage Of EK Specific Probes
	EK		
1	10	59	16.94%
2	2	49	4.08%
3	11	54	20.37%
4	6	68	8.82%
5	10	70	12.82%
6	9	48	18.75%
7	12	53	22.64%

8	5	47	10.63%
9	4	58	6.89%
10	9	47	19.14%
Average	7.8	55.3	14.11%

Table 2. No. of Probes eliciting EK and Percentage of EK elicited in Standard set of Probes

Participants	**Standard**	**Total No. Of Standard Probes**	**Percentage Of Ek In Standard Probes**
	EK		
1	7	59	11.86%
2	11	59	18.64%
3	11	59	18.64%
4	4	59	6.77%
5	8	59	13.55%
6	15	59	25.42%
7	11	59	18.64%
8	9	59	15.25%
9	4	59	6.77%
10	10	59	16.94%
Average	9	59	15.25%

We observed that EK was generated on probes referring to hacking actions and techniques (refer Table 1&2). On average, the subjects elicited 14.11% Experiential Knowledge on Specific Probes and 15.25% in Standard Probes. Thus, we can state that EK can be elicited on Hacking process using the techniques and actions used in the attack for making probes.

Table 3. Paired Sample t-test of EK in Specific and Standard Probes

		Paired Differences				
		Mean	**Std. Deviation**	**t**	**df**	**Sig. (2-tailed)**
Pair 1	**SPECIFIC - STANDARD**	-1.200	3.910	-.970	9	.357

The Paired sample t-test scores between EK of Specific and Standard Probes. On average, Standard set EK scores are 1.200 points higher than Specific set EK scores. The Standard Deviation is noted to be 3.910. The p-value corresponding to the given test statistic *t = -.970* with degrees of freedom *df* = 9 is 0.357(p>0.005). This indicated there was no significance difference between Experiential Knowledge on Standard Hacking process i.e. Phishing as compared to the Specific Hacking experience. This accepts the null hypothesis of the second Hypothesis. (refer Table 3)

Subjects 1, 3, 4, 5 & 10 (Refer Tables 3.1 & 3.2) refer to professional hackers. Anaverage of 15.91% and 13.55% Experiential Knowledge is generated in Professional Hackers on the presentation of Specific and Standard Probes, respectively. Specific Probes elicited slightly high percentage of Experiential Knowledge, when compared to Standard Probes.

Table 4. Paired Sample t-test of EK in Specific and Standard Probes in Group 1

		Paired Differences				
		Mean	**Std. Deviation**	**t**	**df**	**Sig. (2-tailed)**
Pair 1	**SPECIFIC - STANDARD**	1.200	1.643	1.633	4	.178

The Paired sample t-test scores of professional hackers between EK of Specific and Standard Probes. On average, Specific set EK scores are 1.200 points higher than Standard set EK scores. The Standard Deviation is noted to be 1.643. The p-value corresponding to the given test statistic $t = 1.633$ with degrees of freedom $df = 4$ is 0.178(p>0.005). This indicated there was no significance difference between Experiential Knowledge on Standard Hacking process i.e. Phishing as compared to the Specific Hacking experience in the Professional Hackers.This accepts the null hypothesis of the third Hypothesis. (refer Table 4)

Subjects 2, 6, 7, 8 & 9(Refer Tables 3.1 & 3.2) refer to Amateur hackers. An average of 12.60% and 17.11% Experiential Knowledge is generated in the Amateur hackers on the presentation of Specific and Standard Probes, respectively. Standard Probes elicited slightly high percentage of Experiential Knowledge, when compared to Specific Probes.

Table 5. Paired Sample t-test of EK in Specific and Standard Probes in Group 2

		Paired Differences				
		Mean	**Std. Deviation**	**t**	**df**	**Sig. (2-tailed)**
Pair 1	**SPECIFIC - STANDARD**	-3.200	4.658	-1.536	4	.199

The Paired sample t-test scores of amateur hackers between EK of Specific and Standard Probes elicited the p-value corresponding to the given test statistic $t = -1.563$ with degrees of freedom $df = 4$ is 0.199(p>0.005). This indicated there was no significance difference between Experiential Knowledge on Standard Hacking process i.e. Phishing as compared to the Specific Hacking experience in the Amateur Hackers.This accepts the null hypothesis of the fourth Hypothesis. (refer Table 5)

We have observed through the results and analysis of BEOS reports that we can elicit EK on hacking by deigning probes sequentially using the actions and techniques used in the attack. The probes like “I also entered \ after the date and hit enter”, “And typed in ifconfig and clicked enter”, “The link was copied in varwww directory”, “Then I clicked on Exploitation Tools”, “I was redirected to the tracking page”, “I typed in LS for list and hit enter”, “I uploaded a shell in the admin panel”, “IP address was displayed in command line”, “I typed MSFconsole”, “I copied it and pasted on first terminal”, “I could get access after Vulnerability got patched”, “I used Gophish Framework”, “I opened another Google Chrome window”, “I was redirected to AWS deployment page”, etc., which has elicited EK in the subjects show that specific information like typing specific words, specific location where the task is taking place, particular tools being used and also internal processing being witnessed by hacker during the process can be remembered by the hacker. Also, probes like “to php?dept_code=bengali'”, “I typed in 'cd ../var/www'”, “nmap - SV ip address of target”, ”; “php?page=edge.php”, etc., which elicited EK show that even the specific codes used can be remembered and Experiential Knowledge can be triggered using them.

The importance of sequencing is more important when BEOS results of probes in individual cases are to be interpreted. In hacking, an attack has a particular sequence of actions and techniques which needs to be analyzed properly before designing the probes. However, one drawback was observed during the study i.e., about the specificity of the context while BEOS profiling on hacking. Many a times, the processes might involve various actions which are commonly used. This now depends on the efficiency of investigator and the scientific officer conducting the BEOS test. The attack and the electronic evidence must be thoroughly analyzed for more specific actions regarding to that particular attack for effective BEOS profiling.

Our results have shown no significant difference in the Experiential Knowledge between Specific and standard hacking processes. This can actually be more helpful when no electronic evidence, information or traces are found during the investigation, but the kind of attack or breach has been identified. When the attack or breach has been identified, we can use the standard process of that breach or attack to design probes by making it more specific by mentioning exact time (if known), information about the victim’s website and it’svulnerabilities (if known or identified).

CONCLUSION

It was found that Experiential Knowledge of an individual on hacking actions and techniques can be elicited using BEOS profiling by designing the probes using the actions and techniques used in the attack or breach. BEOS profiling can be used in Cyber-crime investigation for screening or pointing out the suspect when the investigation gets difficult due to identification of ownership and authorship to electronic information and evidence collected by analysing the actions and techniques used in the attack or breach and using them in designing the probes for BEOS profiling.Also, when no electronic evidences or tracks are found in an attack but the attack or breach is identified, we can use the standard process of the attack or breach identified to design probes for BEOS profiling along with some specific attack related information.

REFERENCES

[1] McQuade III, S. C. (2006). Understanding and Managing Cybercrime. New York: Pearson Education, Inc.
[2] Hughes, J. (2003). The Internet and the Persistence of Law. Boston College Law Review, 44(2), 359-396
[3] Brenner, S. W. (2008). Cyberthreats: The Emerging Fault Lines of the Nation State. New York: Oxford University Press.
[4] Bocij, P., & McFarlane, L. (2003). Cyberstalking: The technology of hate. The Police Journal, 76, 204-221.
[5] Mutnick, K. D., & Simon, L. W. (2002). The Art of Deception: Controlling the Human Element of Security. Indianapolis, Indiana: Wiley Publishing John Wiley & Sons, Inc.
[6] Mulhall, T. (1999). Where have all the hackers gone? Part 3: Motivation and deterrence. Computers & Security (16), pp. 291-297.
[7] Sudha, S., Mukundan, C. R. (1998). Visual Information in Young, Middle and Elderly Subjects - An Event Related Brain Potential Study. In proceedings of 9th World Congress of the International Organization of Psychophysiology. Taormina, Sicily, Italy. 14-19.13.
[8] Mukundan CR. (2005). Brain electrical oscillation signature profiling for forensic applications. International Conference of Association of Forensic Sciences, 21-26.15.
[9] Akin, T. (2011). Cybercrime: Response, investigation, and prosecution. Encyclopedia of Information Assurance (pp. 749-753). New York: Taylor and Francis.
[10] Davidoff, S., & Ham, J. (2012). Network Forensics - Tracking Hackers Through Cyberspace. Upper Saddle River, NJ: Pearson Education, Inc.
[11] Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and Examining Computer Forensic Evidence. Forensic Science Communications, 2(4).
[12] Brown, C. S. D. (2015). International Journal of Cyber Criminology (IJCC), 9(1), 55–119. DOI: 10.5281/zenodo.22387