ISSN: 2522-3429 (Print)
ISSN 2616-6003 (Online)

International Journal for Electronic Crime Investigation

(IJECI)

Vol. 4(1) Jan - March 2020
ISSUE: Jan. - March 2020

Email ID: ijeci@lgu.edu.pk

Digital Forensics Research and Services Center
Lahore Garrison University Lahore, Pakistan.

LGU International Journal for Electronic Crime Investigation
Vol. 4(1) Jan - March 2020

CONTENTS

LGU International Journal for Electronic Crime Investigation
Vol. 4(1) Jan - March 2020

Sountra et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article | Vol. 4 Issue 1, Jan, - March 2020

STANDARDIZATION OF FORENSIC EVIDENCE ITS PROCUREMENT PRESERVATION AND PRESENTATION IN COURT OF LAW USING FBI TECHNIQUES BY FIA

[1]Prof Dr. Aftab Ahmad Malik, [2] Engr. Mujtaba Asad, [3] Waqar Azeem

1Faculty of Computer Science, Lahore Garrison University (LGU), Pakistan
[2]PhD Scholar, School of Electronics Information & Electrical Engineering,
Shanghai Jiao Tong University, Shanghai China
[3]Assistant Professor, Department of Computer Science (LGU), Pakistan
[1]dr_aftab_malik@yahoo.com, [2]asadmujtaba@sjtu.edu.cn, [3]waqar.azeem@lgu.edu.pk

Abstract

The purpose of this paper is to present the some feasible standards used by US Federal Bureau of investigation (FBI) to enable Federal Investigation Agency (Pakistan) to enhance the authenticity of evidence and its consistency with the existing law. There are examples of several hundred cases, where the courts refused to punish the offender due to unauthentic inconsistent or naive evidence. The investigator is normally responsible to procure and preserve the forensic evidence to strengthen the case of the prosecutor. The investigator has follow up the legal procedure, technically in technically correct manner and consistent with provisions of Law, circumstantial and oral evidence. The inherent deficiencies and faults render the forensic evidence invalid sometimes and no use in the court. The approach of the paper is to standardise and synchronise the working as for as dealing with forensic evidence is concerned. The FBI provides very useful methodologies for procuring evidence from the sconce of offence, forensic services, examination of evidence, rendering forensic evidence,

Keywords: Chemistry forensic examination, Evidence Act, Documentary Evidence

1. Introduction:

This paper deals with highlighting the need for enhancing the quality of forensic evidence by FIA and using the technologies used by FBI. The manpower for effectively handling the tasks involved in collecting, testing and using the forensic evidence is not adequate. The FIA lacks qualified and skilful manpower for the tasks under discussion. A brief resume is presented in section 2 to strengthen the manpower. The present authors have been projecting the important factors regarding effectively presenting the forensic evidence, in various published research papers.

The effective mannerism by prosecutors to support the digital forensic evidence has been discussed in [1] and how to present it in court of law. In [2] a detailed presentation is given on DNA Fingerprints, Facial Prints and other Digital Forensics as Evidence in Criminal Investigation and Court Proceedings to make the prosecution case stronger. The paper [3] prescribes and advocates the "use of codes in place of Fingerprints images during image processing for Criminal Information in large Databases and Data warehouses to reduce Storage, enhance efficiency and processing speed". The facial images also play important role is preserving the criminal information. It is advocated in [4] using an algorithm, to store the

criminal information by means of codes instead of facial images to speed up and enhance the working and capability of criminal Databases and Data Ware houses. The algorithm also reduces the storage requirements and accommodates all particulars of criminal information required efficiently. Another useful algorithm has be designed by [5] which effectively uses codes in place of criminal names in the databases and data warehouses to quickly retrieve the criminal information using unique key like name code. The contribution made in the development of algorithms presented in [6], [7] and [8] makes the storage and retrieval of criminal information from databases using fingerprints and/or criminal appearance must easier and direct.

2. Kinds of Forensic Evidence for processing

Apart from oral and documentary evidence, there are several types of forensic evidence, which are processed and formulated by the investigator for the prosecution. For example the Blood Splatter, DNA evidence, Fingerprints, Ballistics, Autopsies, fibers, firearm residues, photographs or videos photographs, receipts of bank and Entomology. The investigator collects forensic evidence from different sources and different forms, but one has to convert into legally presentable form for court proceedings. For most of the forensic evidence processing require expertise from chemists, biologists or the experts in other field discussed in section 4 of this paper. The inadmissible forensic evidence is of no use in the court of law because [9] such evidence can neither prove nor disprove the facts or circumstances of the case.

The admissibility of evidence has to look into the criteria prescribed and mentioned in PPC and CRPC. In criminal law, the evidence must be capable of proving the offence without any doubt. However, in civil proceeding the case is judged by the "standards of preponderance of the evidence. The authors of this paper are of the opinion that the investigating personnel must prepare the evidence in form which is admissible. According to [10], the document or testimony is admissible in court which can prove the case of prosecution in court of law and is not deviant.

Other important area in preparing the forensic evidence discussed in [11] and [12] is of practical importance; accordingly the expressions used in text must legally be consistent. The oral and signed evidence need to be properly drafted and crafted particularly telephone calls, ransom notes, dying declarations and other items. The description of threats, bribes, conspiracy or perjury must also be carefully represented in the text of the statement. Any inconsistency may render the evidence to be inadmissible. Similarly the wording of Confession, Interrogation, and Deception must also be carefully handled [12].

The important factors while preparation of the forensic evidence, which makes it admissible in court, must be indeed relevant to the case, real, credible, believable and reliable.

Drafting and preparing evidence based on unfair, prejudicial approach, misleading contents which wastes time of court and prosecutor, depend upon "hear say" contents may rendered inadmissible in the court and cannot be used in the court. Therefore the evidence must be analysed and review before presentation in the court.

3. The Role of Forensic Chemistry and Forensic Biology

The forensic Toxicology has been playing pivotal role in conjunction with Forensic Chemistry; similarly the field of Biochemistry is of immense importance in the works related to forensic evidence. The identification and determination of unknown materials is carried out by forensic Chemist using various methods and instruments which a forensic Lab must possess, particularly in FIA.

It is the duty of the Chemist to examine, assess and interpret the chemicals, bullets, explosives, bomb pieces, derbies, powders, liquids, liquors, poisons and toxic materials, stains, other warfare chemical agents and to analyse the physical forensic evidence from crime scene. The chemists do the case working as well as operational tasks i processing the forensic evidence. The chemist also is required to conduct regular research related tasks. The forensic Biologist and Biochemist examine and report fingerprint and DNA samples collected from the scene of offence. In Forensic

Toxicology following ingredients are determined:

- Determination of toxic materials and their effects and effects of alcohol or other drugs,
- Drug tolerance,
- Therapeutic index,
- Carbon monoxide or hydrogen sulphide poisoning and their effects on brain

Certain tasks are performed jointly by Chemist and Biologist.

Figure 1: Forensic experiment in testing Lab

Figure 2: DNA Test in Peshawar Lab

Nowadays some universities offer degrees in criminology with specialisation in Forensic Biology and Toxicology due to the importance of their disciplines. In Australia the Murdoch University is famous in the disciplines such as speciality related to handling areas of Crime Science, White Collar and Corporate Crime. Malaysia also offers elite Forensic Science programs directed towards and focusing on forensic investigations.

The degrees in Biochemistry and Forensic Biology are offered as a normal routine.

4. Squads of FBI to process Forensic Procedures

Federal Bureau of Investigation (BFI) is equipped with strong departments to support the task of investigation. The strongest one are that Chemistry and Biology to cater the processing of Forensic procedures jointly. The Labs at FBI are equipped with most recent equipment to handle all types of Forensic tests and quarries. This is uniqueness with FBI to have all types of experimental Labs and qualified and skilful manpower. The Federal Investigation Agency (FIA) possesses strong legal setup but lacks in strength of the following squad of qualified and experienced man power as possessed by FBI:

Table 1: Role of Experts in formulating evidence

S#	Field	Task
1.	Biologist	To conduct & analyze DNA test of the samples and comparison of DNA Samples.
2.	Chemists	Scientific interpretation, assessment and chemical analysis of physical forensic evidence.
3.	Cryptanalysts	Handle the cryptic communications, records, or symbols and to break the codes, wherever necessary.
4.	Document Analyst	Operational investigations and post-crime forensic analysis regarding the identification and comparison of document
5.	Electronics Engineer	Examination of explosive and other devices having electronic devices; Procuring Computer based codes and information. In collaboration with Computer personnel.
6.	Forensic Operations Specialist	This job offers investigative, technical, operational, and logistical support such as conduct of complex and high-hazard forensic operations.
7.	Geologist-Forensic Examiner	Forensic metallurgy services. Metallurgists within the Laboratory Division conduct metallurgical analysis of materials and provide scientific support to FBI investigations.
8.	Management and Program Analyst	Program analysis and analytical functions using qualitative and quantitative methods to improve the efficiency and effectiveness of work methods.
9.	Metallurgist-Forensic Examiner	Conduct metallurgical analysis of materials and provide scientific support to FBI investigations, scientific assessments, interpretation, assisting in crime scene investigations and providing trial testimony.
10.	Visual Information Specialist	Provide graphic and physical modelling for investigator and prosecutor, Create technical diagrams, demonstrative exhibits and special equipment and apparatus, and forensic facial imaging.
11.	Photographer	Photographer Laboratory, Photographer Scientific and Technical and Photographer Forensic perform tasks

Following are test sample of DNA report reproduced from [13]

Paternity Test Certificate

By order of John Test we were requested to perform a paternity test. Following individuals were examined:

SAMPLE NR.	ROLE	NAME	DATE OF BIRTH
HID123830_001	Alleged Father	Jim Doe	11/11/1990
HID123830_002	Child	John Test	22/02/2012

Regarding the sampling of the participants please refer to the protocols in copy.
We received the originals of the identity confirmations and of the consent statements.
Method:
DNA isolation was carried out separately for all samples. Genetic characteristics were determined by the following PCR-single-locus-technology analysis.
Promega PowerPlex 21 (WEN ILS 500)
With the Promega PowerPlex 21 (WEN ILS 500) twenty one (21) independent PCR- systems were analysed: Amelogenin AM, D3S1358, D1S1656, D6S1043, D13S317, Penta E, D16S539, D18S51, D2S1338, CSF1PO, Penta D, TH01, vWA, D21S11, D7S820, D5S818, TPOX, D8S1179, D12S391, D19S433, FGA.
In parallel, positive and negative controls were performed which gave the expected and correct results.

chaftstests-Briefvorlage-EF-V12_150224

Figure 3(i): DNA Test Sample Report
(Courtesy: Vaterschaftstests-Briefvorlage-EF-V12_150224)

DNA-System	DNA-criteria Jim Doe HID123830_001	DNA-criteria John Test HID123830_002
AM	X, Y	X, Y
D3S1358	14,14	14,18
D1S1656	16.3,17.3	16.3,17.3
D6S1043	11,17	17,17
D13S317	9, 12	9,9
Penta E	10,16	10,16
D16S539	12,12	12,13
D18S51	12,13	13,14
D2S1338	23,23	23,24
CSF1PO	10,11	9, 10
Penta D	9, 10	8,9
TH01	6,6	6,7
vWA	15,17	15,18
D21S11	29,30	29,30
D7S820	8, 11	9, 11
D5S818	11,13	11,12
TPOX	9, 11	9, 11
D8S1179	13,14	13,14
D12S391	18,18	18,19
D19S433	13,14	14,15
FGA	18,25	18,19

Figure 3(ii) Results

Courtesy: Vaterschaftstests-Briefvorlage-EF-V12_150224

Conclusion

It has been emphasised by the authors of this paper in [14] that there must be a connected association between the members of the investigating team and the prosecutor. The collection of evidence, its procurement from the scene of offence, Lab Testing and organisation of information so prepared; all such activities require experts in the concerned areas. The coordination between the Forensic Experts and legal experts is also very much required. Therefore it is strongly recommended that the Federal Investigation Agency (FIA) must take measure to update their own Laboratories and hire competent experts as shown in Table 1 similar to the setup prevalent in FBI.

Acknowledgment:

The authors are grateful for the encouragements by Mr Koukab Jamal Zuberi, the Director DFRSC LGU, Lahore

References

[1] Dr. Aftab Ahmad Malik, Mujtaba Asad and Waqar Azeem (2018), " Effective Prosecution to Support Digital Forensic Evidence During Investigation and Court Proceedings", International Journal for Electronic Crime investigation, ISSN 2522-3429;IJECI; Volume 3 ,April-June 2018; Lahore Garrison University, Lahore.

[2] Dr Aftab Ahmad Malik, Asad and Waqar Azeem (2018); "DNA Fingerprints, Facial Prints and other Digital Forensics as Evidence in Criminal Investigation and Court Proceedings" , International Journal for Electronic Crime investigation, ISSN 2522-3429;IJECI; Volume 2,

Issue :1 ,PP 01-09; January-March 2018; Lahore Garrison University, Lahore.

[3] Dr. Aftab Ahmad Malik, Asad and Waqar Azeem (2018)," Using codes in place of Fingerprints images during image processing for Criminal Information in large Databases and Data warehouses to reduce Storage, enhance efficiency and processing speed", International Journal for Electronic Crime Investigation, ISSN 2522-3429 ; IJECI ; Volume 1, Issue :1 , October-December 2017; Lahore Garrison University, Lahore (Printed and published in 2018).

[4] Dr Aftab Ahmad Malik and Mujtaba Asad (2017), "Algorithm for using Codes in place of facial Images during image processing in large databases/warehouses to reduce storage and enhance efficiency and processing speed"; LGURJCSIT: Lahore Garrison University Research Journal of Computer Science and Technology; Vol 1, Issue 2, April-June 2017, PP:1-9, ISSN 2519-7991.

[5] Dr Aftab Ahmad Malik, Asad and Waqar Azeem (2017), "Algorithm for coding person's names in large Databases / Data warehouses to enhance processing speed, efficiency and reduce storage requirements Lahore Garrison University Research Journal of Computer Science and Information Technology, Volume 1, Issue 1, January-March, 2017; ISSN 2519-7991.

[6] Dr Aftab Ahmad Malik: "Software for Finger Prints Storage and Retrieval of Criminal Identification System for Police", Research Journal, University of Engineering Technology, Lahore, Volume 12; No. 4; PP: 1-18

[7] Dr Aftab Ahmad Malik: Software for Storage and Retrieval of Criminal Information for Police", Research Journal, University of Engineering technology, Lahore, Volume 13; No.1 PP: 1-28

[8] www.legalmatch.com › law-library › article › what-is-admissible-evidence

[10] What is admissible Evidence, published in Legal Match, https://www.legalmatch.com/law-library/article/what-is-admissible-evidence.html

[11] M. Correa, "Forensic Linguistics: An Overview of the Intersection and Interaction of Language and Law," KALB? STUDIJOS; Studies about Languages, Vol. 23, 2013.

[12] Roger W. Shuy (1998), "The Language of Confession, Interrogation, and Deception (p. 2), DOI: http://dx.doi.org/10.4135/9781452229133

[13] www.vaterschaftstests.de

[14] Dr Aftab Ahmad Malik, Mujtaba Asad, Waqar Azeem," Deficiencies in PECA and proposed amendments to facilitate Investigating Agencies, Courts and Prosecution; Proper Use of Electronic Devices for effective implementation of Law; International Journal for Electronic Crime Investigation, ISSN 2522-3429 ; IJECI ; Volume 3, Issue: 3, July-September 2019; Lahore Garrison University, Lahore.

Fatima et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article | Vol. 4 Issue 1, Jan, - March 2020

A Brief Overview of Social Engineering

Muhammad Shairoze Malik
Lahore Garrison University
Shairozemalik@lgu.edu.pk

Abstract:

Right now digitization, the requirement for information protection and information security is very significant. The IT organizations today lean toward their information over everything. Not just for organizations, information security is significant for any person. Be that as it may, regardless of how secure is the organization, how best in class is the technology utilized or what amount cutting-edge their product is, there's as yet a weakness in each segment known as 'Human'. The craft of acquiring sensitive data from a person is known as Social Engineering. Technology has advanced rapidly in recent years, but the danger of Social Engineering still persists in the society. This is mostly due to lack of awareness regarding social engineering attack patterns. Social engineering is an extremely basic practice to accumulate data and touchy information using portable numbers, messages, SMS or direct methodology. Social engineering can be extremely valuable for the aggressor whenever done in an appropriate way. This paper will look into some of the basic and rudimentary techniques used by attackers to gain personal information about victims. The goal of the article is to enable others in successfully defending against social engineering attacks by having the knowledge into how these attacks are performed.

Keywords: Spear Phishing, Pretexting, Watering Hole, Phishing, SEToolkit, Baiting.

1. Introduction:

Generally, the data breaches and information theft in any organization is due to some vulnerabilities present in the organization itself. However, this vulnerability is not only in the technical department. Humans are also considered as a vulnerability as people present in different sectors can also be used to extract confidential information and here comes the word Social Engineering [1]. In digital security, social engineering alludes to the control of people so as to instigate them to complete explicit undertakings or to part with data that can be useful by an aggressor [2]. Social engineering in itself doesn't really require a lot of specialized information so as to be effective. Rather, social designing goes after normal parts of human brain research, for example, interest, politeness, artlessness, sympathy, covetousness, and so on. Social engineering has expanded radically over the most recent couple of years. As indicated by a study, Social Engineering was associated with the 95% of the assaults that occurred in most recent couple of years [3].

2. Social-Engineering Attacks:

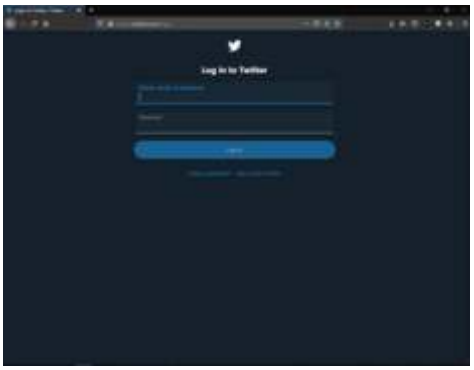
There are many types of attacks are used by malicious hackers to perform social engineering which is explained below. There are basically seven types of social engineering attacks [4, 5]:

1. Phishing:

Phishing is the most widely recognized and compelling approach to accumulate data about the target [6]. Phishing is for the most part done

through emails. These phishing pages generally contain links that redirect the target to some malicious website. Approximately 90% of people using internet receive phishing emails on regular basis. If the phishing has to be done on a specific person, the malicious hacker first tries to find some interest in the target so that the probability of the target clicking on the email increases. The phishing generally focuses on gathering sensitive information of target like social media accounts details, Credit card details etc.

To study this process in more detail let's see the example below in which the attacker makes a fake clone of Facebook Page and when the target enters his credentials in the fake page, the attacker gets all the credentials and the personal information of the target is compromised. The practical below is done using 'Social engineering Toolkit (SEToolkit)'.



(Fig 1. Original Twitter Page)

(Fig 2. Fake Twitter Page)

(Fig 3. Attacker got the credentials)

2. Spear Phishing:

Spear phishing is another type of phishing attack but in this instead of targeting too many people the focus is on a specific person. This method is really hard as compared to a normal phishing attack. In this, the hacker gains information about his target like his likes, dislikes, characteristics etc. It is a time consuming method, where it may take from one week to several months, depending upon the target. Spear phishing is far more effective and efficient way of social engineering as compared to other ways if done professionally. For instance, a hacker sends an email with a critical update to the employees of targeted IT company. The email contains a malicious link which redirects them to a page were hacker either ask them to update their software by downloading a file (which contains malware) or as them to change their password on the malicious page itself and the company's security is compromised [7].

3. Baiting:

Baiting is similar to the phishing attack, but in baiting the attacker promises for something in exchange. For example, the hacker promises free music, phones, prize money, etc. and to get this the target has to just log in to a page or has to share some personal information. Some hackers send infected pen drives to employees of the company as a gift and this flash drive contains malware which is used for hacking into company's network. Baiting is commonly done through emails and adds. Baiting adds are common on unsecured sites and dark web [8]. The screenshot below shows a baiting mail which promises money by clicking on link.

(Fig 4. Baiting Email)

4. Watering hole Attack:

The name watering hole attack is inspired by a real-life situation in which the predator lurks near the water holes so that they can attack a targeted prey. Similarly, in this attack, attacker instead of getting directly in touch with the target the attacker keeps track of every website that his prey visits frequently. Now, the attacker chooses the most frequent website that his target visits. The attacker will then find a vulnerability in this website like reflected XSS, stored XSS, host header, etc. and so that the attacker can fetch confidential data from his target. This type of attacks is really on government employees, as hacking into government sector is really difficult and risky. So, the attacker uses their target's most frequently visited sites to get their personal information like tracking details or any kind of sensitive information. Watering hole attacks are though uncommon but are really dangerous as these attacks are really difficult to detect [9, 10].
Let us assume that the attacker wants to hack into or gather information about Metro, Washington DC. The attacker first chooses a common site where his target visits frequently. The people from three other sectors also visit the same website as shown in the figure. Now the attacker will hack into this common site and the attach some malware, phishing pages, baiting pages, etc. The site is now compromised. Here, instead of attacking all four sectors the attacker will only try to get information of the person associated with Metro. This way, instead of connecting directly to the attacker, an indirect way of gathering sensitive information is attained.

(Fig 5. Working of Watering Hole Attack)

5. Pretexting Attack:

In a pretexting attack the attacker builds up a fictitious scenario in which the possibility of target giving his sensitive information is increased. This method is generally used to trick employees of IT organization so that they give away the personal information of their client like their usernames, passwords, security questions, etc. This information can be used to build further trust relationships with other clients and then used for further social engineering. The small successful steps taken during the pretexting phase is one of the reasons for large data theft and security breaches. The strength of this type of attack totally depends on the awareness and intelligence of the target. If the target is intelligent enough to identify these attacks, then this attack can be prevented. This attack is mostly done through mobile number spoofing. Many IT firms nowadays, educate their employees about these attacks and how to prevent them.

6. Quid Pro Quo:

This attack is similar to the Pre-texting attack but in this, the attacker instead of making random calls, contact the employee of an IT firm to solve any technical issue in their system and network. The attacker first gathers information about the network and systems in the targeted organization. Then the attacker calls an employee of that organization as a technical support, security maintenance charge, etc. Most of the times the employees believe in this and give the information to the attacker [11]. This information may be the Wi-Fi password, username of or maybe they give away the username and password of his own system. This technical information helps the attacker to hack into the system or network and analyze the confidential information. This attack is a really successful attack and the data through this attack is compromised in 70% of the cases.

3. How Social Engineering Effect our lives?

Social Engineering Attacks are currently one of the most damaging attacks on any IT organization. At least 60% of the IT companies were the victim of Social Engineering attacks in 2016 and these attacks kept on increasing by 2017. The leakage of sensitive data of IT firms and their users is one of the biggest threat to social engineering. But, what would an attacker do with this information? So here's the answer,

the personal information of the targets like accounts, credit card details, etc. are being sold on the dark web. At least 70% of the internet is contained in dark web. This information is sold on the dark web at really high prices and then used for illegal purposes. Below are some screenshots which tell us how our personal information is being sold on the dark web [12, 13, 14].

4. Precautions:

1. Different Passwords:
As indicated by a study roughly 60% individuals utilize same passwords for various records which makes simpler for hackers to hack into their records [15].
2. Strong Passwords:
Utilizing solid passwords is one of the essential method for preventing social-engineering attacks. A strong password key must contain a blend of alphanumeric characters.
3. Security Questions:
Using the security questions to verify identity can enhance the overall security of your account. These questions contain private information of users, which are hard to crack [16].
4. Two-Factor Authentication:
Using the two-factor authentication service provided by almost all major websites like Facebook, WhatsApp, Gmail, etc. can enhance the security of accounts.
5. Suspicious/Infected Sites:
Avoid visiting suspicious websites as the may contain infected pages or malicious code by hackers, which can then either compromise your system or steal your personal information [17].
6. Email from Unknown Source:
As most of the phishing attacks are done through emails. So users should avoid opening emails from unknown source as the may contain malicious code or these emails can be used to target users to social engineering attacks.
7. Antivirus:
Antiviruses should be installed, as they can detect the entry of malicious code or file in your system and prevent it from execution thus saving the user from potential loss of data or system compromise.
8. Log off accounts:
Always log off the accounts when they are not in use. This can prevent attackers from hijacking user's accounts and prevent from hacking attempts like session hijacking, cookie injection, etc. [18]
9. Always check the URLs:
One should always check the URL before using the website. The websites which has SSL certificate(HTTPS) installed in them are considered secured.
10. Avoid giving your laptop/smartphone to Strangers:
Preventing any third person from using your phone or laptop is one of the best methods of preventing non-technical social engineering.
11. Never install untrusted apps and software:
Most of the android devices does not have antivirus installed on them. Linux is protected from viruses but malware from there untrusted apps are still a problem.
12. Never insert any unknown flash drive:
Many people attach USB's from unknown places which contain malware and help an attacker to take full control of their system.
13. Change passwords frequently:
One must change his account's password whether it be social media accounts or bank accounts, passwords must be changed frequently.
14. Increasing awareness about Social-Engineering:
One of the best methods to prevent Social Engineering is to educate people about it and how it is affecting our life [19, 20].
5. Conclusion:
In the paper, we looked into multiple social engineering attack patterns which are often deployed by hackers to targets the victims. The effects of these attacks on an organization shows us that how much disastrous social engineering is for society as the leak of private information of individuals effects both their personal and private life. We further listed several possible precautions which can be taken by individuals to help them safeguard their sensitive information form social engineering attacks. The conclusion is that it is difficult to stop social engineering assaults as there is no fix for the human weakness. Teaching individuals about the social engineering and its unfavorable impacts can positively diminish this sort of attacks however can't be completely eliminated.
6. References:
[1] C. Hadnagy, Social engineering: The art of human hacking, Wiley, 2010.
[2] B. Blunden, "Manufactured Consent and Cyberwar," in Proc. LockDown Conference, 2010.
[3] K. D. Mitnick and W. L. Simon, the art of

deception: Controlling the human element of security, Wiley, 2001.
[4] D. P. Twitchell, "Social engineering in information assurance curricula," in Proc. The 3rd annual conference on Information security curriculum development, 2006, pp. 191-193.
[5] N. B. Ellison, "Social network sites: Definition, history, and scholarship," Journal of Computer Mediated Communication, vol. 13, pp. 210-230, 2007.
[6] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," Communications of the ACM, vol. 50, pp. 94-100, 2007.
[7] S. Abu-Nimeh, T. Chen, and O. Alzubi, "Malicious and spam posts in online social networks," Computer, vol. 44, pp. 23-28, 2011.
[8] G. M. Weiksner, B. Fogg, and X. Liu, "Six patterns for persuasion in online social networks," Persuasive Technology, 2008, pp. 151-163.
[9] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites," in Computational Science and Engineering, 2009. CSE'09. International Conference on, 2009, pp. 117-124.
[10] M. Huber, "Automated social engineering, proof of concept," Royal Institute of Technology Stockholm, 2009.
[11] S. T. Thompson, "Helping the hacker? Library information, security, and social engineering," Information Technology and Libraries, vol. 25, pp. 222-225, 2003.
[12] R. Gibson, "Who's really in your top 8: network security in the age of social networking," in Proc. The 35th annual ACM SIGUCCS fall conference, 2007, pp. 131-134.
[13] B. Fogg and D. Iizawa, "Online persuasion in Facebook and Mixi: a cross-cultural comparison," Persuasive Technology, 2008, pp. 35-46.
[14] J. Nagy and P. Pecho, Social Networks Security, pp. 321-325, 2009.
[15] G. Hogben, "Security issues and recommendations for online social networks," ENISA position paper, vol. 1, 2007.
[16] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in Proc. the 2005 ACM workshop on Privacy in the electronic society, 2005, pp. 71-80.
[17] R. G. Brody, "Flying under the radar: social engineering," International Journal of Accounting and Information Management, vol. 20, pp. 335-347, 2012.
[18] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," April 2010.
[19] T. Mataracioglu and S. Ozkan, "User Awareness Measurement Through Social Engineering," arXiv preprint arXiv:1108.2149, 2011.
[20] D. Rosenblum, "What anyone can know: The privacy risks of social networking sites," Security & Privacy, IEEE, vol. 5, pp. 40-49, 2007.

Sountra et al LGU (IJECI) 2019

LGU International Journal for
Electronic Crime Investigation

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

Research Article | Vol. 4 Issue 1, Jan, - March 2020

Bloodstain Pattern: An open source of Evidence A Case Study

Muhammad Rashad Bhatti, Ayesha Sarwar

csifst16@gmail.com ayeshansarwar@gmail.com

Abstract:

The purpose of this paper is to present a case study of a crime committed in a remote area of Pakistan where a woman was found dead and her death was reported as a suicide. Investigation agency collected the data including the pictures from the crime scene. These pictures were sent to crime scene unit for their recommendations. Forensic experts studied and analyzed these pictures and by applying the techniques of Bloodstain Pattern Analysis (BPA). As blood behaves according to certain scientific principles, trained bloodstain pattern analysts can examine the blood evidence left behind and draw conclusions as to how the blood may have been shed. It is done by examining the distribution, location, shape and size of the bloodstains and it helps in determining about what did or did not happen. Because blood behaves according to certain scientific principles, trained bloodstain pattern analysts can examine the blood evidence left behind [and draw conclusions as to how the blood may have been shed]. BPA provides information not only about what happened, but just as importantly, what could not have happened.

A detailed analysis gave enough evidence to the experts that the submitted case was not a suicide rather it was a case of a homicide. The paper will attempt to study the observations of experts while analyzing the bloodstain pattern submitted to them and the conclusions they subsequently drawn, leading towards a clear evidence of a murder case.

Keywords: Bloodstain Pattern: Crime Scene; Suicide; Forensic Evidence

Introduction:

In Pakistan Crime Scene Units work as a support department of investigation agencies like police. They consist of forensic and investigation experts. This paper will attempt to study and analyze a case of femicide wherein a female was found dead in a room of her house. Paper will try to give a detailed analysis of the evidence present on the crime scene, observations of the unit and recommendation given by them. The incident occurred in a tribal area. The incident was reported by the family of the deceased as a case of suicide. Observations made by the unit on the crime scene had indications of manipulation of evidence. Careful systematic observation of the crime scene by the crime scene unit, revealed that in fact the evidence was manipulated. Thus, the Investigating Officer (I.O.) was advised to look into the possibility of a homicide rather than a suicide. On directions of crime scene unit, the husband of the deceased was arrested. The evidence for his involvement was later confirmed by laboratory analysis.

Literature Citation:

Violence against women is one of the most widespread violations of human rights which affects women of all ages, cultures and races. On estimation one out of three women is subjected to

violence in her life. Femicide (Killing of a woman because she is a woman) is the worst expression of this violence. Too often justice is not served due to non-coordination among relevant stakeholders. Every society, country and government seem resolved to make sure that gender-based killings are not to be tolerated and the offender should not go unpunished. This message remains a primary point of concern in trainings and development of everybody working in support of administration of justice in that society. Now forensic evidence is being used extensively in crime scene units to reach the truth and this approach is also proving to be very helpful in solution of gender-based crimes in which, formerly, evidence used to be manipulated by the stakeholders including close family members. The case study under discussion is such a case where evidence was influenced by the family members of the deceased, yet law enforcement agencies were successful in solving the case using the forensics.
Any manifestation or wielding of uneven relationships of power between men and women that culminates in the death of one or more women is considered to be femicide [1]. This type of crime can occur in various situations including: death perpetrated by an intimate partner, serial crimes, sexual violence followed by death, associated femicides or extermination. Murders of women cannot be understood as accidental or pathological: the greatest risk factor is being a woman, and they are killed because they live in patriarchal societies [2].

In various countries, a large proportion of the murdered women had histories of repeated violence and had tried to break up their relationships before being killed, especially during the last three months prior to the crime [3]. Femicide constitutes the most extreme form of violence against women and girls. It occurs in many parts of the world; in fact, few societies are free of it. There are, however, a number of prevalent forms, as stated by the WHO, 'Femicide is usually perpetrated by men, but sometimes female family members may be involved. Femicide differs from male homicide in specific ways. For example, most cases of femicide are committed by partners or ex-partners, and involve ongoing abuse in the home, threats or intimidation, sexual violence or situations where women have less power or fewer resources than their partner' [4].

To external observers, femicide might be interpreted simply as 'senseless violence'; however, this ostensibly 'senseless' condition implicitly denotes and refers to a cultural pattern that has an underlying rationale. The concept of femicide arose specifically in opposition to the 'reasonability' of this extreme form of violence against women not only within patriarchal social systems, but also in any other cultural contexts where it is 'justified'. For the most part, femicides occur in the private sphere, concealed from the public eye. Prevention of these deliberate murders requires they be rendered visible. Traditionally, femicide in the home enjoyed something akin to the principle of nonintervention families as independent republics each home with its own rules; nobody had the right to comment or interfere. However, in many countries, the domestic space is no longer a zone free for privatizing violent behaviors. Since femicide was named, there has ceased to be any place for the inviolability of the home. Femicide overrides the imagery of inviolability [5] and neutrality in the face of this violence.

According to the studies women were most frequently killed by men in the context of heterosexual relationships: by husbands, ex-husbands, partners, former partners, men with whom they were in casual 'on-off' relationships or men they encountered in a dating or sexual context. Combined, men in these categories carried out 63% (n=95) of all femicides [6]. This case study also refers to the same category of femicide.

As with suicide, femicide can be distinguished according to type. It includes so called 'honor' femicides, sex selection before birth, dowry marriage femicides and a host of other manifestations of extreme violence culminating in the death of a woman. Intimate femicide is just one form of femicide perpetrated by a familiar person, usually a family member. It includes murder by intimate partners and killings which occur when a woman is killed by a male family member for dishonoring the family status [7&8]. The term 'honor killings' has been criticized by some scholars [9], who prefer to regard these kinds of murders simply as 'femicides', which should be examined in the wider context of colonization. Intimate partner femicide is the final act of domestic violence or intimate partner violence, and is often the ultimate result of years

of suffered violence. A recent study affirms that 39% of all femicides (and 6% of all homicides) are intimate partner murders; in high-income countries, the percentage rises to 41% of all femicides [10]. As with suicide, rates of femicide vary from year to year and from country to country. Differing rates across regions and cross-national variations have been reported widely [11]. During the period 1985-2010, female homicide victimization increased in some countries in Europe (e.g. Switzerland, and Portugal), remained relatively stable in others (e.g. France and Italy), while countries such as Norway had extremely low rates of femicide. Accounting for macro-level variations in female homicide victimization requires knowledge of socio-political trends, such as post-communism, as well as an understanding of different criminological theories [12]. Like other developing countries, Pakistani society has a patriarchal structure and most of the socioeconomic space is owned and controlled by men. Because of the large gender disparities in the areas of health, education, and economic and political participation, women are usually subordinated to men and are frequent victims of violence. Archer reports that women's victimization rates are generally higher than men's in societies where women have less power and low social status [13].

Bloodstain Pattern Analysis (BPA) studies the interpretation of the shape and distribution of bloodstains connected with a crime. BPA also helps to distinguish between accident, homicide and suicide or to identify bloodstains originating from a perpetrator. Bloodstain pattern examiners typically adopt the terminology recommended by the Scientific Working Group on BPA (SWG-STAIN). Bloodstain patterns are classified into three categories [14]:
passive, transfer and spatter patterns:

- Passive patterns include drip stains, drip trails, drip patterns, low patterns and blood pools and it is normally caused due to the action of gravitational force.
- Transfer patterns are due to blood-bearing surface meets an-other surface Spatter patterns include cast-offs, splash, expiration, projected etc.
- Spatter patterns comprise small and tiny bloodstains which are typically smaller than passive stains.

Bloodstain pattern analysis has been used in criminal investigations for several years. Analysis has been made faster through modern methods of measuring bloodstain patterns. However, since the beginning the basic principles of the analysis and the conclusions drawn have not changed. Bloodstain pattern analysis provides important forensic information about the crime under investigation; it tells what happened. Bloodstain patterns occur in several distinct categories, each revealing a piece of the crime scene puzzle. Crime scene investigators make a series of different measurements on the bloodstains at a crime scene and the data are used to reconstruct what happened during the commission of a crime scene. Every effort must be made to preserve the crime scene until the bloodstain evidence has been investigated. Bloodstain pattern analysis is a powerful tool used in solving violent crimes and must be performed by well-trained individuals. It is one of the most effective methods of reconstructing crime scenes available to forensic analysts [15]. A highly qualified analysis can help to estimate facts concerning the location, quality and intensity of an external force. A sequence of events may be recognized, and detailed questions connected with the reconstruction of the crime might be answered. In some cases, BPA helps to distinguish between accident, homicide and suicide or to identify bloodstains originating from a perpetrator [16]. Analysis of bloodstain morphology can support individualization of stains by directing the selection of a limited number of stains from a complex pattern for DNA analysis. The complexity of real situations suggests a step-by-step approach starting with a comprehensive view of the overall picture. This is followed by a differentiation and analysis of single bloodstain patterns and a search for informative details [17].

A case report of a 72?year?old woman who was found dead in her bedroom with a 4 cm vertical stab wound in the abdomen. A bloodstained knife was found in the top drawer of her bedside table. The clothes worn by the victim showed no damage. A bloodstained vest and a sweater with frontal incisions were found far from the victim, in the bathroom and in the bedroom respectively. Several bloodstains were found in every room of the apartment. The evidence found during the forensic examination and, in particular, the Bloodstain Pattern Analysis, led the investigators to determine the manner of death, being consistent with a suicide with a long?lasting physical activity after self?stabbing. This report

describes an unusual case of "disguised suicide," in which the victim tried to cover?up the suicide by changing her clothes and concealing the weapon, in the last minutes of her life [18]. The mentioned case report refers the phenomenon of disguise or misinterpretation of events leading to conclude the manner of death. This case study is also an example to best describe the factual interpretation of crime scene events based on sound knowledge of bloodstain pattern analysis.

Methodology:

In this paper a qualitative approach was applied to a case using BPA (Bloodstain Pattern Analysis).

Bloodstain pattern analysis (BPA) is the interpretation of bloodstains at a crime scene or at laboratory in order to recreate the actions that caused the bloodshed.

BPA uses principles of biology (behavior of blood), physics (cohesion, capillary action and velocity) and mathematics (geometry, distance, and angle) to assist investigators in answering questions such as:

- Where did the blood come from?
- What caused the wounds?
- From what direction was the victim wounded?
- How were the victim(s) and perpetrator(s) positioned?
- What movements were made after the bloodshed?
- How many potential perpetrators were present?
- Does the bloodstain evidence support or refute witness statements?

Case Study:

Crime Scene Unit FSL now and then deals with several dead bodies at various death and homicide scenes. Deaths with sharp tools often found in homicide cases. Dealing with such dead bodies to extract the physical evidence and to reconstruct the crime scene is quite a technical and frantic task. In this case the CSU team encountered a scenario in which a dead body of a forty (40) year old woman was found in a room (used as a store room) with a knife on her left shoulder, lying supine with legs wide open on the soiled floor of the room. Blood spatter was evident on the face of the victim.

Initially the family (victim's in laws) reported that she committed suicide by cutting through her neck with a household knife in the storeroom (a room in guest portion). The area where the house is situated is rural and has two portions one is for family members and second is the guest portion. The dead body was intact, and the scene was secured to process. A suspected sharp force wound was observed on the front neck beneath the chin of the victim. The presence of dry blood on the face and under the head of the victim assured that the dead body was consistent with the crime scene. Observations of the scene, dead body, and the presence of sharp force wound on front neck and a wooden handle knife (Apparently a kitchen knife) on her left shoulder was not corroborating with statement that she committed suicide due to depression. These observations helped the CSU team in understanding the scenario and collecting the probative evidence related to the homicidal act. All probative evidence items including bloodstains after swabbing and knife (Murder weapon) were photographed, packaged, sealed and documented according to SOPs in order to maintain chain of custody. Buccal swabs were taken as a reference DNA sample of the victim.

Crime Scene Observations

The crime scene unit searched the crime scene thoroughly for evidence and following observations were made:

Figure 1- Entry door of the crime scene room.

Figure 2- Location in room where deceased body was found.

1. Both patterns, bloodstain pattern on the wall and blood pool on the floor are in corroboration with the position of the deceased body right before receiving the injury. Position remained consistent after injury and till the victim became unresponsive. This indicates that the position of the victim was mainly enforced. Moreover, on soil floor surface few deformities indicate very little movement as sign of struggle. A clean void on the opposite end (to the wall) of the blood pool. It led to opine the involvement of minimum two persons in the activity.

Figure 3- Bloodstain Pattern on the wall and Blood pool on the floor.

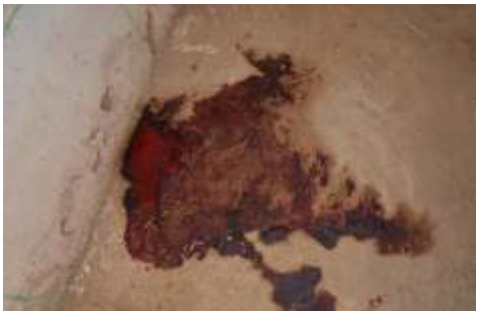


Figure 4- Blood pool on the floor with a clean void on opposite end to the wall.

2. As the bloodstain pattern most probably transferred from assailant's clothing to door surface (swipe pattern) it indicated the movement of individuals from guest portion towards family portion, probability of family members involvement could not be ruled out.

Figure 5 & 6- Swipe Blood pattern on door's surface

3. Knife, murder weapon was having blood on front blade edge (pointed end), corroborating with stab activity. It also describes the position of the assailant sitting on the chest of the victim to induce a single stab in front neck area.

Figure 7- Bloody pointed end of knife

Conclusion:

Based on effective crime scene investigation findings, the crime scene team linked the forensic evidence with the suspect, victim and crime scene. Physical evidence collected from the scene turned out to be helpful in revealing the truth in the homicide incident and on crime scene team recommendations, police arrested the victim's husband. Later the one suspect (victim's husband) confessed to the crime and court convicted him with capital punishment based upon evidence while his accomplice (brother of suspect) is still on the run.

The study shows an immense need to strengthen system of collection and analysis of mortality

data, which includes the physical data from the crime scene and its forensic interpretation and analysis. This will help equip and empower the law enforcement agencies to gather evidence that may help the institutions responsible for administration of justice. This information can assist the investigator in reconstructing the crime, corroborating statements from witnesses, and including or excluding potential perpetrators from the investigation.

This study also confirms that the absence of forensic facilities in remoter areas help the perpetrator of a crime to escape from responsibility, and more in the cases when the perpetrators are in a position of authority thus able to influence the facts of the case by manipulating the evidence.

For academic purpose only one streak of evidence that is the bloodstain pattern has been analyzed in current study showing that conclusive evidence can be extracted from a single or alternatively form several sources. At times the conclusion achieved analyzing certain facts is a fruit of a poisonous tree and thus not admissible in a court of law. But nevertheless, it would help in giving the investigators and direction to work unto.

Data (the pictures of the crime scene) was collected by professionals and its chain of authentications were maintained, thus these findings were presented in the court of law and were an important evidence on which the decision of the case was made.

References

1. A. Carcedo & M. Sagot, "Femicide in Costa Rica 1990-1999", Pan American Organization of the Health, Washington, 2000.
2. A. Carcedo, "We neither Forget nor Accept". Femicide in Central America, 2000-2006. ISBN 9789968851275 9968851272.San Jose, CEFEMINA, 2010.
3. S.J. Grana, "Socio-structural considerations of domestic femicide". J. Fam.Violence, v.16, n.4, p.421-35, 2001.
4. World Health Organization (2012) Understanding and addressing violence against women. Available at: www.who.int/reproductivehealth/topics/violence/vaw_series/en/ (accessed 1 February 2016).
5. LC. McClain, "Inviolability and privacy: The castle, the sanctuary, and the body", Yale Journal of Law and the Humanities Vol.7, 2016.
6. Femicide Census Report, UK, 2018.
7. A. Gill, C. Strange & K. Roberts,"Honor' Killing and Violence: Theory, Policy and Practice", Basingstoke: Palgrave Macmillan, 2014.
8. A. Sever, "Patriarchal Murders of Women: A Sociological Study of Honor-based Killings in Turkey and the West. Lewiston", NY, Edward Mellen, 2013.
9. N. Shalhoub-Kervorkian, & S. Daher-Nashif, "Femicide and colonization: Between the politics of exclusion and the culture of control", Violence against Women Vol. 19(3), pp 295-315, 2013.
10. H. Stockl, K. Devries & A. Rotstein, et al. "The global prevalence of intimate partner homicide: A systematic review", The Lancet 382, pp. 859-865, 2013.
11. C. Corradi, & H. Stockl, "Intimate partner homicide in 10 European countries: Statistical data and policy development in a cross-national perspective", European Journal of Criminology Vol. 11(5), pp. 601-618, 2014.
12. J. Stamatel, "Explaining variations in female homicide victimization rates in Europe", European Journal of Criminology Vol. 11(5), pp. 578-600, 2014.
13. M. Nasarullah, KJ. Cummings & S. Haqqi, "The Epidemiological patterns of honor killing of women in Pakistan", European Journal of Public Health. Vol. 19(2) pp. 193-7, 2009.
14. Scientific Working Group on Bloodstain Pattern Analysis. Standards and Guidelines, Recommended Terminology, 2009.
15. Doug Hanson, "Bloodstain Pattern Analysis: Redirecting the scene of crime", Law Enforcement Technology, Vol. 31, Issue.2 pp. 84-90. 2004.
16. O. Peschel, S.N. Kunz & E. Mutzel, "Blood stain pattern analysis", Forensic

Science, Medicine & Pathology, Vol. 7, pp. 257-270.
17. B. Karger, S. Rand, T. Fracasso & H. Pfeiffer, "Bloodstain Pattern Analysis-Casework Experience", Forensic Science International, Vol. 181, Issue. 1-3, pp. 15-20, 2008.
18. Guido Pelletti M.D, Sindi Visentin M.D, Claudio Rago M.D, Giovani Cecchetto M.D & Massimo Montisci M.D, "Alteration of the Death Scene After Self?stabbing: A Case of Sharp Force Suicide Disguised by the Victim as a Homicide", Journal of Forensic Sciences, Vol. 62, Issue. 5, pp. 1395-1398. 2017.

Fatima et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article | Vol. 4 Issue 1, Jan, - March 2020

Body Language Detecting Deception

Fatima Fatima
fatima.dfrsc@lgu.edu.pk
Lahore Garrison University

Abstract

The objective of this review paper is to discuss the understanding of body language deception. This study explains a detail interpretation of body language also known as nonverbal cues including facial expressions called micro-expressions and other bodily moves of speakers/suspects during interviews and investigation process. It will emphasize on importance of reading body language in criminal investigation for lie detection and proper training of investigators/interviewers for an effective interrogation. It explains proper documentation of nonverbal cues and recording them for further assistance in multiple interviews in future as these cues remain for a short time. It will enlighten the effects of gender, social and economic status on body language and their resulting cues. A proper knowledge and training of reading nonverbal behaviors can increase forensic application of body language in criminal justice system for the identification of the right guilty party.

Keywords: Body Language, Lie detection, Interpreting Nonverbal Cues, Criminal Investigation.

1. Introduction

Words when spoken contained all the thoughts and feelings which usually walk off unsaid and fail to set out their way through the vocal tract as in verbal form of communication (1&2). Scientists agree on one thing that how fast we process thought, i.e. we think much faster than we speak. Brain processes the thought and our body visibly reacts faster before we think of what we want to say about that thought. Even before anything being said, our body will give away to our answers (5&17). Therefore, this type of body reaction can deceive the individual who wishes to keep their thoughts and feelings as secret. This reaction or language is said as non verbal communication normally known as 'body language' and its interpretation is called Kinesics (1, 2&4). All parts of the body such as facial expressions, head, eyes, arms and legs etc. are involved in non verbal communication (1, 2&11). Some studies have shown that kinesics or body language accounts for 60 to 65% (19&21) and some for 55-95% of all communication (4). Such as an investigator may observe a subject lying if its words and body language or kinesics do not agree (4&5). When talking about body language, we go for a slight indication or cue that is sent and received to each other nonverbally (18). Body language of people around us whether at office, out with friends or during an interrogation speaks volume. Like from facial expressions, eye behavior to the direction in which body moves or a person points his or her feet, reveals what a person is really thinking and the things we don't say can still suggest volumes of information (19&20).

People tell lies and betray of varying degrees in every day experiences with closely linked action and emotion (8&16). For a deceiver to lie, it requires him to keep facts straight, making story believable and hold up scrutiny (13). Usually a suspect says all the truth or right things without making a single slip of tongue during an interview but it is his/her body language that will clue that he/she is lying (1). While individual make every effort when they tell truth to ensure that people understand whereas liars try to manage people's opinion. As a result, people unconsciously signal deception via non verbal cues (9&13). Shakespeare said, 'guiltiness will

speak though tongues were out of use' (1). Similarly like fingerprint cues are for eternity even if they are not entirely evident. However, in contrast with fingerprints, cues from body language can possess more than one association which should not be misinterpreted. Body language cues as evidence are different from that of physical pieces of evidence as these are not carefully preserved to be filtered by analysts in the lab. Body language during an interview can be recorded for an expert to review but with very less opportunity to hold up and distinguish the evidence which body language can present (1&5).

Body language is helpful even for a layman to understand if someone is honest or truthful, or hiding something back. But it would be more effective for a trained person in recognizing and understanding of body language (1&8). In some situations, recognition and understanding become critical such as within criminal justice system. In criminal investigation, interpretation of body language can provide constructive base in determining the direction that will take (1, 4&6). For a productive investigation, body language can be useful if approached with suitable care in recognizing certain physiological responses with a range of emotional sources. Its proper use can assist police officer and guide jury members as they listen to the suspects and witnesses during interviews respectively (1&7). It is important for officers to get an expert literacy in this reference as they manage the investigation and are in frequent contact with witnesses and suspects. Proper training can ensure the accuracy in interpretation of body language. In criminal justice system, this accuracy is not negligible thing if the purpose is to discover the truth and to protect the citizen by ensuring that no innocent is mistakenly convicted, and to identify the guilty. But unfortunately, this necessary training is often neglected and officers rarely get advance education in nonverbal communication after they leave police academy (1&5).

2. Understanding Body Language

Body language is a non verbal form of communication between two or group of individuals which consists of physical behaviors such as body posture, gesture, limb movements, facial expressions and eye movements (2, 6&7). All such behavioral signals are sent and interpreted by humans entirely subconsciously. Clue from the body language is the result of attitude or state of mind of a person. Like it may present aggression, thoughtfulness, boredom, relaxed state, pleasure, laughter, and intoxication etc. (2&4). Factually body language is an involuntary action of body parts as physical expression. It does not have grammar like other languages and is broadly interpreted by other people (6&7). Physical expressions like waving, pointing, touching and slouching are all integral forms of non verbal communication (2).

Researches have shown that humans move their bodies when communicating as it makes the mental effort easy when communication is difficult. This movement of the body is termed as body proximity (10&18). The physical movements reveal many signs about a person like gestures can pass on a message or highlight a point, posture shows boredom or interest and touch can express care or support. It should be noted that some signs of emotions like smiling or laughing when happy and frowning or crying when sad, are chiefly universal. These basic emotions included a range of positive and negative emotions, and all of these are not encoded in facial muscles. According to Ekman, newly list of encoded emotions includes amusements, contempt, embarrassment, contentment, excitement, guilt, pride, relief, satisfaction and shame (2&4). Other than these physical expressions and emotions, body ornaments and embellishments are all extensions of our body language such as cloths, jewelry, sun glasses, hairstyles etc. Where certain colors and styles send signals, interaction of humans with their body ornaments also gives indication of relationship, and culture and religion origin. Like fidgeting with watch or ring, self preen and touching hair, are all body language cues (18).

3. Principles of Interpreting Body Language

Reading body language or nonverbal cues has been noticed for centuries. It has become center of attention for researchers and practitioners in many fields such psychology and forensic investigation. For over twenty five years, it has been subjected to intensive scientific study.

Lawyers have just begun to realize the importance of reading body language or nonverbal behavior, and how long others have known. Reading body language is frequently used to understand people, their perception, nature of communication and relationship between them (1, 2&7).

Humans use many forms of deception using facial expression as it is a very complex and easily manipulated form of communication. To detect deceptive behavior, depends largely on the ability of investigators that how they observe and differentiate human behavior. Cluster of behavior which supports the deceptive behaviors specific to the person interviewed, should be identified. Investigators should know how to formulate questions that could facilitate behavioral observations. Greater number of observations will result in greater probability of detecting deception (11&13). Few things must be kept in mind to have an effective behavioral analysis or reading body language as following:

3.1. Understanding the Baseline Body Language

To read body language of a person, observers or investigators should understand the baseline body language they are interviewing. Knowing the reaction of a person in calm state will help to observe changes in body language when being questioned during an interview. However, if an investigator is unfamiliar with the interviewee, spending time and discussing non threatening topics would help to understand the baseline behavior and communication style of interviewee for later comparison when the situation becomes more intense (17&22). Like some people are proverbial open book while some are not easily decoded (3&13). Behavior and interpretation of behavior can be affected by the influence of culture and ethnicity. Environmental circumstances and situations can also influence on the display of the communication being surrounded. Therefore, it is very significant to observe the clustering of behaviors as it tells more than a single reaction and visualizes the magnified behavior carefully that would help to decode it (10&3). These behavioral samples can be used by inexperienced investigators as reference for comparing with deceptive behaviors (13).

3.2. Watch for Nonverbal Cues

Nonverbal cues can identify a person if being deceptive. According to experts, one such most common cue is doing something to give time to think of an answer. For example, coughing or taking drink. That few seconds the person takes to cough or drink, gives him/her sufficient time to come up with an answer that might not be truthful (5&6). Other signs/cues that show state of being not completely truthful are shifting seats, not being able to make eye contact and all that body language that disagrees with words such as nodding head yes while saying no. In this situation, interviewers should be careful and trained to read body language because it is very risking to assume a person is lying only if he or she takes time to drink/cough. In over all investigation, body language should be data point and combined with all other relevant information to make a decision (17).

3.3. Gaze at Facial Expressions

Face is the index of mind and facial expression conveys more signs than other part of the body (2). Face is an important reference point to interpret nonverbal cues. It is common courtesy to look someone in face when speaking so face receives a lot of attention. Facial statements are more verbose than the words being spoken for those people who believe on what face tells rather than what they hear. People commonly look in the face and eyes for deception cues if they suspect any falsehood (1, 2&4). A wise liar can control his facial expression but one can still pick up important nonverbal cues by paying close attention to face (1, 14&19). One can put on fake smile on his/her face when actually feeling unhappy or holding up a blank face when panicking internally. It is possible that people would see these falsified expressions but traces are always left behind on the face which cannot be erased even how a liar is good to manage his/her facial expression. These invisible facial changes are significant and last only for less than 10-15 seconds, called micro expressions. One within criminal justice system, either a police officer or investigator or a District Attorney should be trained enough to read these timely facial expressions and body language (1&15).

The face and short facial gestures or micro expressions are the window to the soul. Every

human makes micro expressions when they feel intense emotions. Micro expressions are essential part of the body language and we are pinched to understand someone's hidden emotions by looking and observing the face. Research studies found that while making the facial expression, we may begin feeling the emotion ourselves. Thus, not only emotions cause facial expressions but facial expressions can also cause emotions. According to psychology researcher Dr. Paul Ekman, there are 7 universal micro expressions which are widely used and easy to interpret (18&30) as following:

3.3.1. Surprise Micro-expression

Surprise look lets know others what exactly we are surprise about. In surprise state, the eyebrows are raised and curved, horizontal wrinkles are formed across the forehead, white of the eye becomes dominant and eyelids are opened, skin below brow is stretched, jaw is open without tension or stretching of the mouth (14,15,20&30) as shown in following facial expressions:

Figure 1: Surprise Micro-expression (30).

1.1.1. Fear Micro-expression

Fear is the state of being scared and closely similar to shock. It indicates to see any threats nearby. When a person is scared, the mouth opens, the eyes widen, and it prepares for a state where one may need to shout for help and to breath in a large amount of oxygen which will be helpful to fight enemy or to run away. As said earlier that not only emotions cause facial expression but facial expression also causes emotions (14&15). Similarly, if seeing someone frightened, we may have been frightened too. Fearful facial expression is the result of activity that takes part in amygdale, a part of our brain. Fear expressions included; eyebrows are raised and drawn together in a flat line, wrinkles are formed in the center between the eyebrows, upper eyelid is raised and lower lid drawn up in tense state, the upper white of the eye is showing, mouth is open with lips slightly tensed or stretched and drawn back (20&30) as in following facial expressions:

Figure 2: Fear Micro-expression (30).

1.1.1. Disgust Micro-expression

Disgust expression appears when smelling something bad or hearing something nasty. In disgust behavior, the eyes are squinted which helps to increase visual activity and to find the origin of disgust. In disgust expressions, eyes are narrowed, upper eyelid, upper lip and cheeks are raised, upper teeth are exposed, and wrinkles are formed on nose (20,21&30) as shown in following expressions:

Figure 3: Disgust Micro-expression (30).

1.1.1. Anger Micro-expression

People with angry facial expression are found less trustworthy. In angry expression, the squinted eyes and lowered eyebrows makes it harder to see the window to the soul, and leads to lower level of trust. People genuinely angry may try to hide their angry expression in social situations therefore anger is stronger social norm violation than any other negative emotions like sadness. However, researchers found the angry expressions are fastest to be detected thus helping to avoid possible physical harm. Angry expressions are with lowered and drawn eyebrows with vertical lines between them, wide or bulging eyes, lips pressed together with corners down, jutting of lower jaw and dilated nostril (20, 21&30) as in following angry expressions:

Figure 4: Anger Micro-expression (30).

3.3.5. Happiness Micro-expression

Happiness expressions show positive and negative feelings and emotions just like a smile on our faces when meeting someone shows interest as a positive sign and turning face to opposite side shows a negative sign. A broad smile during communication expresses comfortable position. Smile is an important nonverbal facial cue. There are more than 50 different types of human smiles and over 80 facial muscles are involved in smiling (2&4). Researchers analyze movements of these facial muscles to tell when a smile is true or fake. A smile is probably fake if it uses only mouth as shown in figure 5 (a) while it is genuine when engaging the whole face as shown in figure (b) (2&19). Genuine smile shows that the person is happy and a fake smile is just to convey pleasure but actually showing that the person is feeling something else (19). Half smile engages only one side of the mouth showing sarcasm or uncertainty, tight pursed lips indicate displeasure whereas relaxed mouth indicates positive attitude and mood (19). Other happy micro-expressions included are lips with corner drawn back and up, parted mouth with exposed teeth, wrinkles running from outer nose to outer lip, raised cheeks, lower eyelid with wrinkles, and crow's near the outside of the eyes indicating genuine smile (20,21&30) as shown in following expressions:

Figure 5: Happiness Micro-expression, a) genuine smile & b) fake smile (30).

3.3.6. Sadness Micro-expression

Sadness is one of the hardest micro-expressions to fake and to correctly identify because it is not very large or noticeable. Similar to surprise, sadness is one of the longer-lasting micro-expressions that even a resting sad face can be developed. This facial expression is a key way to calm down those who are angry. Sadness expressions include contracted and raised inner eye brows, skin below the eyebrows is up with inner corner and triangulated, lip's corners are drawn, lower lip pouts out, and raised jaw (15,20,21&30) as in following expressions:

Figure 6: Sadness Micro-expression (30).

3.3.7. Contempt/Hate Micro-expression

Contempt is similar to hate and is a negative feeling of dislike, disrespectful or being offensive towards someone. It is the only micro-expressions which is asymmetrical. It gives the feeling of superiority over another, and rightness and bad impression of someone being contempt. In contempt behavior, mouth is raised from one side (15, 20, 21&30) as shown in following expressions:

Figure 7: Contempt Micro-expression (30).

3.4. Read the Eyes

Of human morphology, eye can be very informative behavior that communicates more than any other part (19&20). It is the most important expression that communicates when the brain conducts internal dialog, recalling past events, crafts answers or processes information (13&19). Eyes give the revealing and accurate communication signals as they are a focal point on the body (2&19). When evaluating body language or nonverbal communication, pay attention to the following eye signals:

3.4.1. Eye Gaze

Observe the person either making direct eye contact or looking away. Direct eye contact

during conversation indicates interest and attention. While making indirect eye contact by looking away or to the sides indicates disinterest, boredom or deceit. On the other hand, looking down is an indication of nervousness or obedience. However, direct eye contact for a long time can feel threatening. Breaking eye contact and repeatedly looking away is a sign of discomfort, distraction and a try to conceal the feeling (19, 20&21). Most of the investigators heavily rely on eye contact and researches show that frequent liar actually increases eye contact because they learned that investigators determine the truth or genuineness by strong eye contact (12&13).

3.4.2. Pupil Size/Dilation

Pupil dilation shows the favorable response or focus towards someone or something being liked. It is difficult to detect the dilation but under the right condition one should be able to spot it. In normal condition, light level controls the dilation while emotions can also cause changes in pupil size. Such as a phrase 'bedroom eyes' is used to describe the look that a person gives when attracted to someone. Similarly highly dilated pupil indicates interest or arouses (19, 20&21) as shown in following figure:

Figure 8: Pupil Dilation (21).

3.4.3. Blinking

Blinking of the eyes speaks about internal ongoing conditions and it is increased when people think more or are stressed. Increased blinking rate accompanied by touching mouth and eyes indicates lying (19&20). Usually rapid eye blinking or eyelid flutter indicates a sensitive topic as shown in figure 9. Officers should be careful while observing the speaker's eyes as they alert deception chances (2&13).

Figure 9: Eye blinking (20).

3.4.4. Glancing

To glance at something suggests a desire for that thing such as glancing at the door indicates a desire to leave or glancing at a person shows a desire to talk to him or her. During conversation, looking upwards or to the right indicates a lie while looking upward but to the left indicates the truth. Looking upward and to the right gives them time to concoct a story using their imagination, and looking upward and to left gives time to recall an actual memory (19&20). Different glancing is shown in following figure:

Figure 10: Eye glancing (20).

3.5. Mouth and Breathing

People attempt to breathe faster with series of short breaths followed by one long deep breath when they want to conceal information. This irregular pattern indicates increased anxiety level of the speaker to the investigator (11&12). Stress causes dry mouth which leads to frequent clearing of throat, cracking of the voice, jumping of the Adam's apple or laryngeal cartilages, a feature of human neck. Similarly, a tense mouth with pursed lips indicates extreme distress which signifies that speaker is preventing him/herself emotionally, verbally and physically (13&21) as shown in following figure:

Figure 11: Pursed lips (21).

3.6. Watch the Head Movement

Head is the first and foremost part of human body that moves to indicate the presence or absence of patience in a speaker. Slow move or nodding indicates interest and spirit to continue talking while fast nodding indicates that the speaker has enough talk or he/she wants to finish speaking or wants him/her turn to speak (2&3). Tilting head sideways shows sign of interest or disapproval or negative mood of speaker, tilting backward shows sign of suspicion or uncertainty, and up and down side shows sign of friendliness and receptive mode. Keeping head straight and level both vertically and horizontally indicates confidence or assurance or sign of authority (12). Pointing head towards people also shows feeling of an affinity. Many researches and brain imaging show that emotions expressed by dynamic head as compared to faces, bring out greater activation in social corner of the brain (13&19).

3.7. Look at Arms and Legs

The arms and legs movement can also be helpful in signaling nonverbal information. An arm crossing is a sign of being defensive and a leg crossing away from a person is an indication of dislike or discomfort. Slight expending of the arms widely is an attempt to look more commanding while keeping them close shows an effort to withdraw from attention (2&3). When evaluating the body language, pay attention to the following arms and legs signals:

- Moving legs around a lot shows the signs of nervousness, stress and deceptive.
- Keeping of one leg ahead and the other in loose position is a sign of leisure environment.
- Crossed arms and legs indicate cold response or reaction.
- Sitting position in which legs are kept over another, is an indication of being ready for a reaction, and shows authoritativeness.
- Sitting on chair and keeping legs over one another with back touched on chair, shows comfort and relaxation as in following figure:

Figure 12 (a): Different legs positions (20).

- Placing hands on the hips in standing position is a sign of ready, control or aggressiveness as in following figure 12 (b).
- Holding hand behind the back can be an indication of feeling bored, anxious or angry.
- Tapping fingers repeatedly or fidgeting shows that a person is impatient or frustrated (13, 19&21).

Figure 12 (b): Different arm positions (21).

3.8. Pay Attention to Body Posture

Posture refers to how one holds body or overall physical form. Body posture serves as an important part of body language by conveying volume of information about feelings and personality characteristics such as confidence, openness or submissiveness. Postures are most reliable of all nonverbal signals to read deception because these are consciously less controlled than other signals (2,12&21). Sitting up straight indicates that the person is focused and pays attention to what so ever is going on. On the other hand, sitting with body curved forward can mean that the person is indifferent or bored. When understanding a body language, try to observe the signals that a person's posture can display as following:

- Open body posture is holding trunk or body chest open and exposed indicates friendliness, openness and willingness.
- Closed body posture keeps the trunk of the

body curved forward, and arms and legs crossed indicating hostility, unfriendliness, and anxiety as shown in following figure (2&21).

Figure 13: Closed and open posture (21).

3.9. Body Proximity

Body proximity defines the body movement in space and the distance between two individuals. Body movements are instrumental body language cues by giving signs of preferences and nervousness (1, 18&19). Close proximity is level of physical distance (6-18 inches) which is best indicating close relationship or greater comfort between the individuals usually during intimate contact like hugging, whispering or touching. Personal distancing (2-4 feet) shows bonding between family members or close friends with affinity and intimacy as shown in figure 14. On the other hand, social distancing is backing up or moving away from someone when comes closer indicating that connection is not mutual. Proximity is not always an accurate sign of affinity with someone because some cultures prefer less or more distancing during interaction (4, 19&21).

Figure 14: Body proximity or individual distancing (20).

3.10. Watch if Someone is Mirroring You

Mirroring is the mimicking or copying other person's body behavior when interacting. Mirroring someone body language is a sign of comfort and establishing a bond with that person as expressed in following figure 15. Such mirroring signs include taking sips of a drink at the same time with the other person and copying the other person who is sitting at a table and resting an elbow on the table (3&19).

Figure 15: Mirroring (19).

3.11. Watch for Pacifying Behavior

Investigators should not be convinced of any one cue or reaction being an absolute sign of deception as there are many theories and myths. There are certain signs of anxiety that may indicate signs of lying when occur together. These physical signs of anxiety are also known as adaptors used to relieve stress as following:

- Internal adaptors show crossing and uncrossing of arms/legs.
- Object adaptors indicating signs of dissipating anxiety by picking up objects and putting them down when the discussion/conversation turns to a comfortable point.
- Self adaptor shows signs of touching body or face (12&23).
-

3.12. Check the Answer, Timing & Voice Characteristics

Evaluate the nonverbal signs with verbal answers. Notice if a person is using harsh or soft terms, answers extended or focused, includes or omits him/her from suspicion, giving direct or non relevant answers to the questions. During interview or conversation, check the time and consistency either a person answering on time or taking time to think before answering or if thinking when he/she should not. Observe voice tone if it goes up or down or remains medium.

Notice the speech if it is clear or mumbled and when accused voice remains neutral or volume increases (12&22).

4. Documentation of Body Language

Documentation is a key to record and pay attention to a body language during an investigation or interview and is as important as listening to verbal cues. Noticing body language when talking can help investigators to understand the whole picture. Such as recording of previous body language interview during an investigation with multiple interviews, helps to understand the focus areas in later interviews (11&12). Making notes about devious eyes or hesitation before answering, results another data to think in the overall investigation. Sometimes verbal answers are not definitive as whether someone is being deceptive or not but paying attention to nonverbal cues is indicating that more questions should occur. Observing and picking up these hints can help to understand their role in sketching the overall depiction which will make the decision in the next step (17, 28&29).

5. Effects of Gender, Social and Economic Status on Body Language

Gender differences can have influence on body language in humans which can be noticed at every state of behavior. It is believed for females that they show signs of higher sensitivity to nonverbal cues. Females with or without Asperser's syndrome characterized by significant difficulties in social distancing and nonverbal communication, are more adept than males in discriminating and recognizing facial emotions and friendliness from sexual interest. In contrast to males, females tend to better recognize emotions from facial expressions than from voices (2&5).

Social and living standard can affect verbal and nonverbal behavior. A rural person way of using body language differs from that of urban area such as rising of hands, walking and movement of body. According to researchers, such behavior may be the reason of poor standard in rural person and superiority complex in an urban person. On the other hand, body language of economically sound person is authoritative as compared to economically unsound person who gives a sign of request (2).

6. Forensic Application of Body Language

As a single body gesture cannot be interpreted apart from overall interaction therefore an experienced and trained investigator or interviewer should observe the whole conversation by picking out cues to focus upon. Areas where discomfort or possible deception observed can lead the interview to a focus point (3&29). In an interview where spoken words are important, nonverbal behaviors also give much information, if not more. Using this knowledge, law enforcement agents can successfully interview the suspects, victims and witnesses. While setting up and conducting an interview, it should be a planned, conscious and even a rehearsed event to extract most effective information. Additionally in the court when agent testifies, officers should be aware of their behaviors and the judges and juries should also interpret behaviors they see (3, 25&28).

Researches, seminars and workshops are constantly being conducted on nonverbal behaviors to develop this skill with devoting professional journals and books. One may spot a liar by paying close attention to physical behavior. According to a German philosopher 'Friedrich Nietzsche' who wrote that 'the mouth may lie but the face it makes nonetheless tells the truth'. Devices are available to detect lies such as the polygraph that detects the stress about the lie but not the lie. By doing so it can miss the most dangerous liars who don't care when they are lying thus showing no stress during a polygraph test (3, 26&27).

7. Conclusion

It is concluded that body language is a mean of interaction and mirror of personality development in society. Body language can be helpful to read mentality of people for a successful interaction. It gives cues about mental attitude, physical fitness and ability of people, and their intention. Healthy perceivers can discriminate between deceptive and true information from body movements for better understanding of people. As the clues are left on the crime scene, similarly clues are left on the face of the guilty person who is trying to assert his/her innocence when close to being discovered. These clues can be in various forms either as frowns on forehead or movements of

arms. It is possible that an innocent person may engage the nervous behavior as those who are actually lying. Therefore, it is important for law enforcement professionals to have training in interpretation of body language and facial expressions to properly identify the real culprit for the well being of our society. With increased interest and application of training in this field accompanied with criminal justice system, is a lead to a room in the future of criminal investigation for a field which is as fascinating as its importance.

8. References

[1] A.K. Gardner, 'Though Tongues Were Out of Use: The Body Language of the Guilty,' Acupuncture & Electro-Therapeutics Research, Vol. 40(2), pp. 101-136.

[2] V.P.Singh, 'Language & Body Language,' Govt. P.G. College, Jalesar, Etah U.P.

[3] C. Stephens, 'Nonverbal Communication,' Journal of Personality and Social Psychology, 2007.

[4] D. Luciew et al,. 'Finding the Truth: Interview and Interrogation Training Simulations,' Inter-service/Industry Training, Simulation and Education Conference (I/ITSEC), 2011.

[5] M.E. Kadar, 'Introduction to Profiling: The Process of Reading of Nonverbal Signs,' Journal of Media Research, Vol. 10, Issue. 1(27), pp.70-87, 2017.

[6] Positive Body Language, 'Tutorials Point: Simply Easy Learning, 2016. Available: www.tutorialspoint.com

[7] Investigative Interviewing for Criminal Case, Convention against Torture Initiative (CTI) Tools 1, 2017.

[8] J.L. Barkai, 'Nonverbal Communication from the Other Side: Speaking Body Language,' Speaking Body Language San Diego Law Review, Vol. 27: 101, 1990.

[9] M. Schollum, 'Review of Investigative Reviewing,' Office of the Commissioner of Police New Zealand, ISBN 0-477-10011-2, 2005.

[10] Allan & B. Pease, 'The Definitive Book of Body Language,' Pease International, 2004.Available:www.peaseinternational.com.

[11] S.B. Walters, 'Practical Kinesics Interview & Interrogation: A Basic Guide,' Psychological Kinesics Interview & Interrogation, 2013. Available: www.TheLieGuy.com

[12] J. Navarro, 'The Dictionary of Body Language,' Digital Edition, ISBN: 978-0-06-284686-0, 2018.

[13] J. Navarro & J. Schafer, 'Detecting Deception,' 2019. Available: www.all-about-body-language.com

[14] J. Endres & A. Laidlaw, 'Micro-expression Recognition Training in Medical Students: A Pilot Study,' BMC Med Educ. Vol. 9, 2009. Available: www.all-about-body-language.com

[15] H.Langfeld, 'Judgment of Facial Expression & Suggestion,' 2019. Available:www.all-about-body-language.com

[16] C.D. Jasmin, 'Good and Bad in the Hand of Politicians: Spontaneous Gestures during Positive and Negative Speech,' the Public Library of Science (PLoS) Vol. 5(7), 2010. Available: www.all-about-body-language.com

[17] D. Muller, 'Work Place Investigations and the Power of Body Language, 2017.Available:https://www.hracuity.com/blog/workplaceinvestigations-and-the-power-of-body-language

[18] Body Language: What is it and how to read, Science of People? Available: https://www.scienceofpeople.com/body-language/

[19] How to Read Body Language - Revealing the Secrets behind Common Nonverbal Cues, Fremont College, 2019.Available:https://fremont.edu/how-to-read-body-language-revealing-the-secrets-behind-common-nonverbal-cues/.

[20] A Forensic Psychology's Guide to Body Language, Forensics College, 2020.Available:https://www.forensicscolleges.com/blog/resources/forensic-psychologists-guide-to-body-language.

[21] K. Cherry, 'Understanding Body Language & Facial Expression,' Behavioral Psychology, 2019. Available:https://www.verywellmind.com/understand-body-language-andfacial-expressions-4147228

[22] J. Bowden, 'Quickly read, analyze, and interpret body language,' 2014. Available:https://www.policeone.com/investigations/articles/quickly-read analyze-and-interpret-body-language-zRM4VIGAUxxcwQkC/

[23] D. Lomer, 'Body Language: How to detect Deception in Investigation Interviews,' 2020. Available: https://i-sight.com/resources/ebook-how-to-detect-deception-in-investigation-interviews-body-language/

[24] Investigative Interviewing: Nonverbal Communication, 2016. Available: https://www.slideshare.net/taproot_rca/investigative-interviewing-nonverbal-communication-64838994

[25] T. Buckhoff* & J. Hansen, 'Interviewing as a 'Forensic-type' Procedure,' Journal of Forensic Accounting, Vol.3, pp. 3-16, 2002.

[26] V. Denault et al,. 'The Analysis of Nonverbal Communication: the Dangers of Pseudoscience in Security & Justice Contexts,' Anuario de Psicología Jurídica, Vol. 30, pp. 1-12, 2020.

[27] E. Sanow, 'The Reid Technique of Interviewing and Interrogation,' Law & Order, 2011. Available: www.lawandordermag.com

[28] R.S. Martin, 'The Importance of Nonverbal Communication in the Courtroom,' Eastern Communication Association Convention, New Haven, CT, 1993.

[29] A. Gurbiel, 'The importance of the body language and the nonverbal signals in the courtroom in the criminal proceedings: The outline of the problem,' World Scientific News, Vol. 112, pp. 74-84, 2018.

[30] 'The Definitive Guide to Reading Micro-expression (Facial Expression),' Science of People. Available: https://www.scienceofpeople.com/microexpressions/#can-you-read-facial-expressions

Sountra et al LGU (IJECI) 2019

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

LGU International Journal for
Electronic Crime Investigation

Research Article | Vol. 4 Issue 1, Jan, - March 2020

Man in the Middle - Hacker's Playground

[1]Shariq Malik, [2]Muhammad Shairoze Malik
[1]Shariqmalik@lgu.edu.pk, [2]Shairozemalik@lgu.edu.pk
Lahore Garrison University

Abstract

There has been an increase in potential sources of threats to the security of information systems and data of governments, companies and individuals in the present day, due to the growing number of information systems types and devices, the expanding availability of freely-downloadable open source tools, the degree of interconnectivity made possible by the internet, and the concentration of more self-help power in the hands of individual end users. A numerically-insignificant number of the total population of information systems end users is made up of black hat users who have caused significant economic losses and reputational damages for organizations and governments through exploitation of security vulnerabilities. One of the most common and widespread security threats is that of Man-in-the-Middle (MitM), which has remained a major source of concern to security professionals for many years, and continues to pose a threat to information security as the focus of attack continues to be data, and the black hat users continue to look for new ways to circumvent security safeguards implemented for existing technologies and countermeasures planned for new and emerging technologies. Many papers have been written about Man-in-the-Middle attack, that have described different kinds of such attacks and explained solutions to the attacks but not illustrated how the attack can be carried out and showed how the risks arising from such attacks can be mitigated. This paper presents a step-by-step account of one way in which MitM attack can be realized and how the confidentiality and integrity of data can be prevented from being compromised through use of PKI (Public Key Infrastructure).

Keywords: MitM (Man-in-the-Middle), Attack, Defense, PKI (Public Key Infrastructure), Security.

1. Introduction

Man in the Middle (MitM) attack refers to a security scenario in which the direct communication of information between two systems is intercepted by a third party who can then secretly passively read, relay and or maliciously modify the data that is being sent between the two communicating systems. The name Man-in-the-Middle is believed to have been coined from a pattern of play in the sport of Basket Ball, whereby two players are in the process of passing a ball to one another while a player between them attempts to seize the ball. It is also referred to as bucket (or fire) brigade attack, which is a name derived from the fire brigade process of putting out fires by passing buckets of water around different persons between the source of the water and the fire. MitM attack is also known as TCP Session Hijacking.

In this report, based on our demonstration of a MitM attack and defense, and limited review of a few relevant research publications, we:

i. Discuss some techniques used in MitM attacks
ii. Present complete instructions to demonstrate a MitM attack.
iii. Present complete instructions to demonstrate a Public Key Infrastructure (PKI) defense against a MitM attack.
iv. Present a conclusion from our observations.

2. Some Techniques used in MitM Attacks

One common feature of all types of MitM attacks is that the attacker forces a

connection to be established with each of the two communicating systems, without the two communicating systems knowing that they are each connected directly with the Man-in-the-Middle and not with each other, as shown in Fig. 1.

2.1 ARP Spoofing

ARP Spoofing is a security attack in which an attacker sends falsified ARP (Address Resolution Protocol) messages across a LAN (Local Area Network), resulting in the mapping of the attacker's MAC address to the IP address of a system or server on the network. It is also known as ARP Cache Poisoning. After the attacker's MAC address has been successfully mapped to an IP address, any data addressed to the IP address will be received by the attacker.
To effectively become a Man-in-the-Middle between any two systems via ARP Spoofing, the attacker will map the IP addresses of the two systems to its system's MAC address.
ARP Spoofing is possible only in LANs that use ARP.

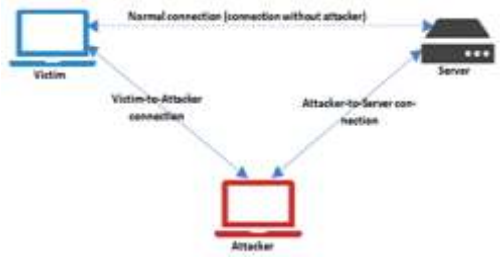
2.2 DNS Spoofing

DNS Spoofing is a security attack in which falsified Domain Name System (DNS) data is injected into the cache of the DNS resolver, causing the DNS to serve the false or fake IP address in response to DNS queries for the affected domain name. It is also known as DNS Cache Poisoning.

The fake address can quite easily spread from one DNS server to several other DNS servers, as other DNS servers query the corrupt DNS cache for the corrupt domain name entry and update their own caches in turn with the falsified mapping.

2.3 Host File Modification

Host File Modification is a security attack in which the attacker successfully fraudulently inserts an entry in the hosts file of the victim's system to map attacker's IP address to a domain name, so that every request sent by the victim to the domain name will be directed to the attacker's system.



(Fig. 1: Man-in-the-Middle Attack)

The attacker can then, in addition to other actions, modify the message's source IP to attacker's IP address and destination IP to the server's IP before sending the message to the server. The server will then send the response back to the attacker, who can then read and or modify the payload and change the source and destination IP addresses to the attacker's and victim's IP addresses respectively before sending the message to the victim.

3. MitM Demonstration

3.1 Demonstration Environment and Tools
The demonstration environment and tools include the following components:
i. Oracle Virtual Box
ii. Three Ubuntu 16.04 LTS 32-bit Linux VMs, namely Server VM, Victim VM, Attacker VM

3.2 Setup and Execution

i. Create three (3) VMs, namely Server, Victim, Attacker
a. Configure Network as Host Only, so that the VMs can communicate with each other but not with the internet
ii. Start the VMs
a. Notice that the VMs have internal IPs in the same network subnet

3.3 Demonstrate Normal Connection (Connection Without Attacker)

3. Do the following in Server's VM:
   a. Create directory, TestServer, in user's home directory:mkdir ~/TestServer

   b. Change directory to TestServer:
   cd ~/TestServer

   c. Create a file inside TestServer directory,

called Mitm.html, that contains just the words "Hi from Server":

```
echo "Hi from Server" > Mitm.html
```

d. Run the following command while in ~TestServer; this command starts a Python HTTP server listening on port 8000

```
python -m SimpleHTTPServer
```

4. Do the following in Victim's VM:

a. Enter the following line inside Victim's /etc/hosts file, to help in resolving www.lgu.edu.pk to the server's IP (replace Red entry below with the server's IP):

```
<Server_IP> www.lgu.edu.pk
```

b. Launch a browser

c. Type the following in Victim's browser and observe that the resulting web page displays the words "Hi from Server":
http://www.lgu.edu.pk:8000/TestServer/Mitm.html

3.4 Demonstrate Victim-To-Attacker Connection

5. Run the following in Victim's VM, to forward all outbound traffic with destination ports 80, 443, 8000, to Attacker's IP (replace Red entry below with the attacker's IP):

```
sudo iptables -t nat -A OUTPUT -p tcp --dport 80 -j DNAT --to-destination <Attacker_IP>
sudo iptables -t nat -A OUTPUT -p tcp --dport 443 -j DNAT --to-destination <Attacker_IP>
sudo iptables -t nat -A OUTPUT -p tcp --dport 8000 -j DNAT --to-destination <Attacker_IP>
```

6. Do the following in Attacker's VM:

a. Create directory, TestServer, under user's home directory:

```
mkdir ~/TestServer
```

b. Change directory to TestServer:

```
cd ~/TestServer
```

c. Create a file inside TestServer directory, called Mitm.html, that contains just the words "Hi from Attacker":

```
echo "Hi from Attacker" > Mitm.html
```

d. Run the following command while in ~TestServer; this command starts a Python HTTP server listening on port 8000

```
python -m SimpleHTTPServer
```

7. Refresh the browser session on Victim's VM and observe the displayed content change to "Hi from Attacker". This is because in Victim's VM, we are now forwarding all outbound traffic going to port 8000 to Attacker VM.

3.4 Demonstrate Attacker-To-Server Connection

8. Run the following in Attacker's VM, to forward all incoming traffic with destination ports 80, 443, 8000, to server's IP (replace Red entry below with the server's IP):

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination <Server_IP>
sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination <Server_IP>
sudo iptables -t nat -A PREROUTING -p tcp --dport 8000 -j DNAT --to-destination <Server_IP>
sudo iptables -t nat -A POSTROUTING -j MASQUERADE
```

9. Refresh the browser session on Victim's VM and observe the displayed content is "Hi from Server". However, the traffic between Victim and Server is now being routed through the Attacker.
10. Open Wireshark in Attacker VM to inspect traffic flow between Victim and Server. The words "Hi from Server" were displayed in plain text.

3.5 Demonstrate PKI Certificates Implementation - A Defense Against MitM Attack

Do the following on Server VM:

11. Copy this file, /etc/ssl/openssl.cnf, to your home directory on Server VM:

cd
cp /etc/ssl/openssl.cnf .

12. Create files and directories under your home directory for openssl, as follows:
mkdir demoCA
mkdir demoCA/certs
mkdir demoCA/crl
touch demoCA/index.txt
mkdir demoCA/newcerts
echo 1000 > demoCA/serial

13. Run the following command to create create CA certificates. You will be prompted for the items shown below following the command:
openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf

PEM passphrase: <Enter a phrase of your choice, but you must remember it>
Country Name: <Enter:- CA>
Province: <Enter:- Ontario>
Locality Name: <Optional, press Enter to continue>
Organization Name: <Enter:- Group4 6100G Project>
Organizational Unit Name: <Optional, press Enter to continue>
Common Name: <Enter:- www.grp4_6100g_project_uoit.edu>
Email Address: <Optional, press Enter to continue>

14. Run the following command to generate public/private key pair. You will be prompted for the items shown below following the command:
openssl genrsa -aes128 -out server.key 1024

passphrase for server.key: <Enter a phrase of your choice, but you must remember it>

15. Run the following to create a CSR. You will be prompted for the items shown below following the command:
openssl req -new -key server.key -out server.csr -config openssl.cnf

passphrase for server.key: <Enter the same phrase you entered when generating public/private key pair above. e.g. fessam>
Country Name: <Enter:- CA>
Province Name: <Enter:- Ontario>
Locality Name: <Optional, press Enter to continue>
Organization Name: <Enter:- Group4 6100G Project>
Organizational Unit Name: <Optional, press Enter to continue>
Common Name: <Enter:- www.grp4_6100g_project_uoit.edu>
Email Address: <Optional, press Enter to continue>
A challenge password: <Optional, press Enter to continue>
An optional company name: <Optional, press Enter to continue>

16. Run the following command to generate signed certificate. Respond to the prompts shown below following the command:
openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf

Sign the certificate? [y/n]: <Enter y>
1 out of 1 certificate requests certified, commit? [y/n] <Enter y>

17. Put both the secret key and the certificate in a .pem file
cat server.key > server.pem
cat server.crt >> server.pem

18. Create and save a script file in user's home directory, named server.py, with the following contents:

```
#!/usr/bin/python

import BaseHTTPServer, SimpleHTTPServer
import ssl

httpd = BaseHTTPServer.HTTPServer(('<Server_IP>', 8000), SimpleHTTPServer.SimpleHTTPRequestHandler)
httpd.socket = ssl.wrap_socket (httpd.socket, certfile='server.pem', server_side=True)
httpd.serve_forever()
```

19. Start Python's secure web server, as follows. Enter the same PEM passphrase as chosen earlier above:
    python server.py

20. Enter the following line inside Victim's /etc/hosts file if not already done, to help in resolving www.lgu.edu.pk to the server's IP (replace Red entry below with the server's IP):
    <Server_IP> www.lgu.edu.pk

21. Launch a broswer on Victim's VM and enter the following as URL. Note that this URL is now using secure HTTP, i.e. HTTPS:
    https://www.lgu.edu.pk:8000/TestServer/Mitm.html

22. If the browser displays error, import the self-signed CA certificate (ca.crt) into the browser, as follows if using Firefox Web Browser (follow the appropriate procedure if using a different web browser), then click Import button:
    Edit -> Preference -> Privacy & Security -> View Certificates

23. Repeat step #21 above, if you did step # 22.

24. Open Wireshark in Attacker VM to inspect traffic flow between Victim and Server.
The words "Hi from Server" were no longer displayed. This is because the contents of the conversation between the victim and the server have now been encrypted and can therefore neither be seen in plain text nor identifiable in Wireshark.

4. Results

From the above demonstration we can take a look at how easy it is for hackers to perform a Man in the Middle attack on a given target and go through the target's sensitive information. In article two types of attacks were demonstrated. One where the traffic between victim and internet in unencrypted while the other in which the said traffic in encrypted. In both cases MitM attack was performed but due to encryption in second attack the sniffed data was not compromised.

5. Conclusion

Man in the Middle attack is just one of the recipes in a hacker's playbook and we can see just how much effective it is in different environments. We can see that without the proper secure certificates implemented on the websites, all the data that goes through them is at risked to be taken. The implementation of PKI certificates effectively protected the integrity and confidentiality of the information exchanged between the victim and the server.

6. References

[1] Mauro Conti, Senior Member, IEEE, Nicola Dragoni, and Viktor Lesyk "A Survey of Man In The Middle Attacks"
IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, THIRD QUARTER 2016

[2] Mayank Agarwal, Santosh Biswas, and Sukumar Nandi "Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks"
IEEE COMMUNICATIONS LETTERS, VOL. 19, NO. 4, APRIL 2015

[3] Matthew Johnson, Peter Lutz, and Daryl Johnson, Rochester Institute of Technology "Covert Channel using Man-In-The-Middle over HTTPS"
International Conference on Computational Science and Computational Intelligence, Year: 2016, Pages: 917 - 922

[4] Enrique de la Hoz, Rafael Paez-Reyes, Gary Cochrane, Ivan Marsa-Maestre, Jose Manuel Moreira-Lemus, Bernardo Alarcos "Detecting and Defeating Advanced Man-In-The-Middle Attacks against TLS"
2014 6th International Conference on Cyber Conflict, Pages: 209 - 221

[5] Prerna Arote and Karam Veer Arya (ABV-Indian Institute of Information Technology and Managament, Gwalior, India) "Detection and Prevention against ARP Poisoning Attack using Modified ICMP and Voting"
International Conference on Computational Intelligence & Networks, 2015, Pages 136 - 141

[6] Peng Zhou (1School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, People's Republic of China), Xiaojing Gu (2School of Information Science and Engineering, East China University of Science and Technology, Shanghai, People's

Republic of China) "HTTPAS: active authentication against HTTPS man-in-the-middle attacks"
IET Journals, 2016, ISSN 1751-8628
[7] Parth Patni, Kartik Iyer, Rohan Sarode, Amit Mali, Anant Nimkar (Department of Computer Engineering, Sardar Patel Institute of Technology, University of Mumbai, Mumbai, India - 400053) "Man-in-the-Middle Attack in HTTP/2"
International Conference on Intelligent Computing and Control (I2C2), 2017
[8] Shaun Stricot-Tarboton, Sivadon Chaisiri, Ryan K L Ko (Cyber Security Lab, University of Waikato) "Taxonomy of Man-in-the-Middle Attacks on HTTPS" 2016 IEEE TrustCom/BigDataSE/ISPA, Pages: 527 - 534
[9] Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. Int. Arab J. e-Technol., 1(2), 26-36.
[10] Altunbasak, H., Krasser, S., Owen, H., Sokol, J., & Grimminger, J. (2004, November). Addressing the weak link between layer 2 and layer 3 in the Internet architecture. In Local Computer Networks, 2004. 29th Annual IEEE International Conference on (pp. 417-418). IEEE.
[11] Anagreh, M. F., Hilal, A. M., & Ahmed, T. M. (2018). Encrypted Fingerprint into VoIP Systems using Crypto-graphic Key Generated by Minutiae Points. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCI-ENCE AND APPLICATIONS, 9(1), 151-154.
[12] Andersen, D. G., Balakrishnan, H., Feamster, N., Koponen, T., Moon, D., & Shenker, S. (2008, August). Account-able internet protocol (aip). In ACM SIGCOMM Computer Communication Review (Vol. 38, No. 4, pp. 339-350). ACM.
[13] Hossain, M. S., Paul, A., Islam, M. H., & Atiquzzaman, M. (2018). Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks. Network Protocols and Algorithms, 10(1), 83-108.
[14] Hudaib, A. A. Z. (2014). Comprehensive Social Media Security Analysis & XKeyscore Espionage Technol-ogy. International Journal of Computer Science and Security (IJCSS), 8(4), 97
[15] Li, X., Li, S., Hao, J., Feng, Z., & An, B. (2017, February). Optimal Personalized Defense Strategy Against Man-In-The-Middle Attack. In AAAI (pp. 593-599).
[16] 'man-in-the-middle-attack" (Rapid Web Ser.), Blog Post, 2017, Retrieved from: https://www.thess-lstore.com/blog/man-in-the-middle-attack/
[17] 'man-in-the-middle-attack-mitm' (Techpedia), 2018, Retrieved from: https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm
[18] 'man-middle-attack' (CA Tech.), 2018, Retrieved from: https://www.veracode.com/security/man-middle-attack

LAHORE GARRISON UNIVERSITY

Lahore Garrison University has been established to achieve the goal of excellence and quality education in minimum possible time. Lahore Garrison University in The Punjab metropolis city of Lahore is an important milestone in the history of higher education in Pakistan. In order to meet the global challenges, it is necessary to touch the highest literacy rates while producing skillful and productive graduates in all fields of knowledge.

VISION

Our vision is to prepare a generation that can take the lead and put this nation on the path to progress and prosperity through applying their knowledge, skills and dedication. We are committed to help individuals and organizations in discovering their God-gifted potentials to achieve ultimate success actualizing the highest standards of efficiency, effectiveness, excellence, equity, trusteeship and sustainable development of global human society.

MISSION

At present, LGU is running Undergraduate, Graduate, Masters, M.Phil. and Ph.D. programs in various disciplines. Our mission is to serve the society by equipping the upcoming generations with valuable knowledge and latest professional skills through education and research. We also aim to evolve new realities and foresight by unfolding new possibilities. We intend to promote the ethical, cultural and human values in our participants to make them educated and civilized members of society.

Contact: For all inquiries, regarding call for papers, submission of research articles and correspondence, kindly contact at this address:
Sector C, DHA Phase-VI Lahore, Pakistan
Phone: +92- 042-37181823
Email: ijeci@lgu.edu.pk

Published by: Digital Forensics Research & Service Center, Lahore Garrison University