International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 11 (November 2014), PP.77-81

Analysis of Existing Models & Proposed Cyber Crime Investigation Model

Dr. Ajeet Singh Poonia
Associate Professor, Department of Computer Science and Engineering
Govt. College of Engineering and Technology, Bikaner, India.

Abstract:- In current scenario cyber crime is increasing at exponential rate, as the technology is growing at enormous speed hence the cyber crime investigation is becoming a tedious job without a proper framework. There is a wide range of different types of cyber crime today which are prevailing in the society. Solution of each case requires is a complicated task. Till date the investigation models proposed by various researchers have some or the other shortfalls. They are somehow limited to certain types of cyber crime only and these models largely restrict themselves to the investigation of the crime scene and the evidence, and so are less extensive in their scope. These models provide overview of the general technical investigation activities. In this paper, a model has been proposed, named "cyber crime investigation model" which will capture a full scope of an investigation process and provide framed activity for every step. The proposed model focuses more into efficiency, accuracy and how to preserve the fragile evidence, its transport and storage.

Keywords:- Cyber Crime Investigating Model, Realization phase, Authorization phase, Audit planning, Auditing, Managing evidence, Hypothesis, Challenge analysis, Dissemination.

I. INTRODUCTION

There are several useful discussions found throughout the studies and reviews that examine and compare many models and frameworks of cyber- crime investigation.The models provide a useful overview of the general technical investigation activities.

Most of the existing model design does not show the information process flow focusing on issue such as chain of custody. The largest gap in most of the presented model is, no attention has been paid on the delicate evidence and also on data acquisition process. For that there should be a proper methodology and procedure to be followed by forensic investigator who focuses more into efficiency, accuracy and how to preserve the fragile evidence. Main concern for the investigator should be for the fragile evidence because this is not like normal evidence during an investigation.

Also the existing model doesn't fully describe the investigation process in a way which will assist the development of new investigative techniques or any innovative methodology which can be implemented for any type of case.

II. CRITICAL ANALYSIS OF EXISTING MODELS

Many of the existing cyber crime investigation models are abstract in the context of law enforcement investigation and are largely restricted to the examination of a definitive technical crime scene and the forensic recovery of digital evidence from established sources. While many of the existing models can be seen to build upon each other by extending earlier approaches with the aim of becoming more complete and robust.

Many of the digital forensic investigation processes have been developed either by traditional forensic scientists focusing on robust evidence handling or by technologists focusing on digital evidence capture, making it difficult for law enforcement practitioners to understand and apply.

The major limitation of existing cyber crime investigation model is that it refers only to the forensic part of an investigation and issues such as the exchange of information with other investigators are not addressed.

The existing models do not cover all aspects of cyber crime investigation; they are not general enough to describe fully the investigative process in a way which will assist the development of new investigative tools and techniques.

Another drawback with the existing models is that they have given more stress on the collection and examination of the evidence, which is basically middle stage of the model. However, the earlier and later stages must be taken into account for a successful cyber crime investigation model, and in particular if all the relevant information flows through an investigation are to be identified.

Transport and storage of digital evidence are still at a basic level. Dissemination is understood to be important but is still limited.

Result analysis of approx all the models along with the inventor and the year of invention have been reviewed here as mentioned in table 1.1.

Model Name	Inventers	Years
Computer Forensic Process	M.Pollitt[1]	1995
Generic Investigation Process	Palmer[2]	2001
Abstract Model of the Digital Forensic Procedures	Reith ,Carr, & Gunsh[3]	2002
An Integrated Digital Investigation Process	Carrier & Spafford[4]	2003
End To End Digital Investigation	Stephenson[6]	2003
Enhance Integrated Digital Investigation Process	Baryamureeba & Tushabe[7]	2004
Extended Model of Cyber Crime Investigation	Ciardhuain[8]	2004
Hierarchical ,Objective Based Framework	Beebe & Clark[9]	2004
Event Based Digital Forensic Investigation Framework	Carrier & Spafford[4]	2004
Investigation Framework	Kohn , Eloff ,& Oliver[10]	2006
Computer Forensic Field Triage Process Model	K.Roger,Goldman,Mislan,Wedge & Debtota[11]	2006
Investigation Process model	Freiling & Schwittay[12]	2007

Table 1.1: Details of the models developed from 1995 to 2007

III. DRAWBACKS OF SOME OF THE MODEL SHOWN IN THE TABLE ARE DISCUSSED HERE:-

The collection of evidence typically occurs after it has been recognized, but in the model proposed by the U.S. Department of Justice (DOJ), shows that it is collected before the digital data have been examined. In this model, collection phase more accurately collects the physical evidence and the digital evidences are collected when they are examined.

In the model proposed by Lee et al., the barrier of the model is analyzing part of digital forensic process only, this have made a limitation in the digital forensic investigation, as not be focusing on the data acquisition neither preparation nor presentation.

In case of Gary L Palmer, model the framework does not dictate what particular actions must be pursued. Instead, it provides a list of candidate techniques, some of which are required. The specifics of the framework must be largely redefined for each particular investigation.

The model proposed by Séamus Ó Ciardhuáin, covers the processes from collection of digital evidence to presentation in court. However, the model does not cover the respective human resource with specific technical and legal experience required for respective processes. Moreover, current models are deficient in explaining about establishment of digital forensic setup at national level to cater for services of all end users. Casey also places a major concern of the forensic process on the investigation itself.

Reith et al. themselves have noted the absence of any explicit mention of the chain of custody in their model. This is a major flaw when one considers the different laws, practices, languages, and so on which must be correctly dealt with in real investigations. It is important to identify and describe these information flows so that they can be protected and supported technologically, for instance through the use of trusted public key infrastructures and time stamping to identify investigators and authenticate evidence.

The Beebe and Clark model provides structure for activities through phase's con- sisting of multiple sub-phases rather than activity groupings. Sub-phases are objective based rather than strictly activity based. The objective based sub-phases each fall into a particular phase and consists of a hierarchy of particular activities that are subordinate to the particular objective.

The studies shows that how exponentially the cyber crime is growing as compare to the conventional crime and how much the available security structure is self sufficient to defend or we can say fight against the cyber crime. So to cope with the situation we have to come with a model i.e. a cyber crime investigation model which covers the gap with the existing models in the system, as discussed above, so as to control or lower down the exponentially growing cyber crime in the system.

IV. DEVELOPMENT OF IMPROVED CYBER CRIME INVESTIGATION MODEL

By this time digital forensic investigation processes are developed by conventional forensic scientists focusing on evidence handling and also developed technical persons focusing on digital evidence capture. This tradition way makes it difficult for law enforcement practitioners to understand and apply. A new model is required to be developed to accommodate all aspects of handling and capturing forensic and digital evidence involved into the cyber crime. After studying and finding limitation in above mentioned cyber crime investigation models a new improved model is required.

In this paper, a model has been proposed, named “cyber crime investigation model” which will capture a full scope of an investigation process and provide framed activity for every step. The proposed model attempts to improve upon existing models through the combination of common techniques while trying to ensure method shortfalls are addressed. It is applicable to all current digital crimes, as well as any unrealized crimes of the future.

The proposed model focuses more into efficiency, accuracy and how to preserve the fragile evidence, its transport and storage. This model describes a framework of activities with flow of information in proper way so that each step suggests a predefined task to complete. Main concern for the investigator is on the flow of information of the model. Auditing phase provides various tools and activities for investigation. This model allows technical requirements for each phase to be developed and for the interaction between physical and digital investigations to be identified. The model can be used in a practical way to identify opportunities for the development and operation of technology to support the work of investigators, and to provide a framework for the capture and analysis of requirements for investigative tools and technologies as they emerge and become the subject of investigations. The proposed model can also provide a unified structure for case studies/lessons learned materials to be shared among investigators, and for the development of standards, conformance testing, and investigative best practices.

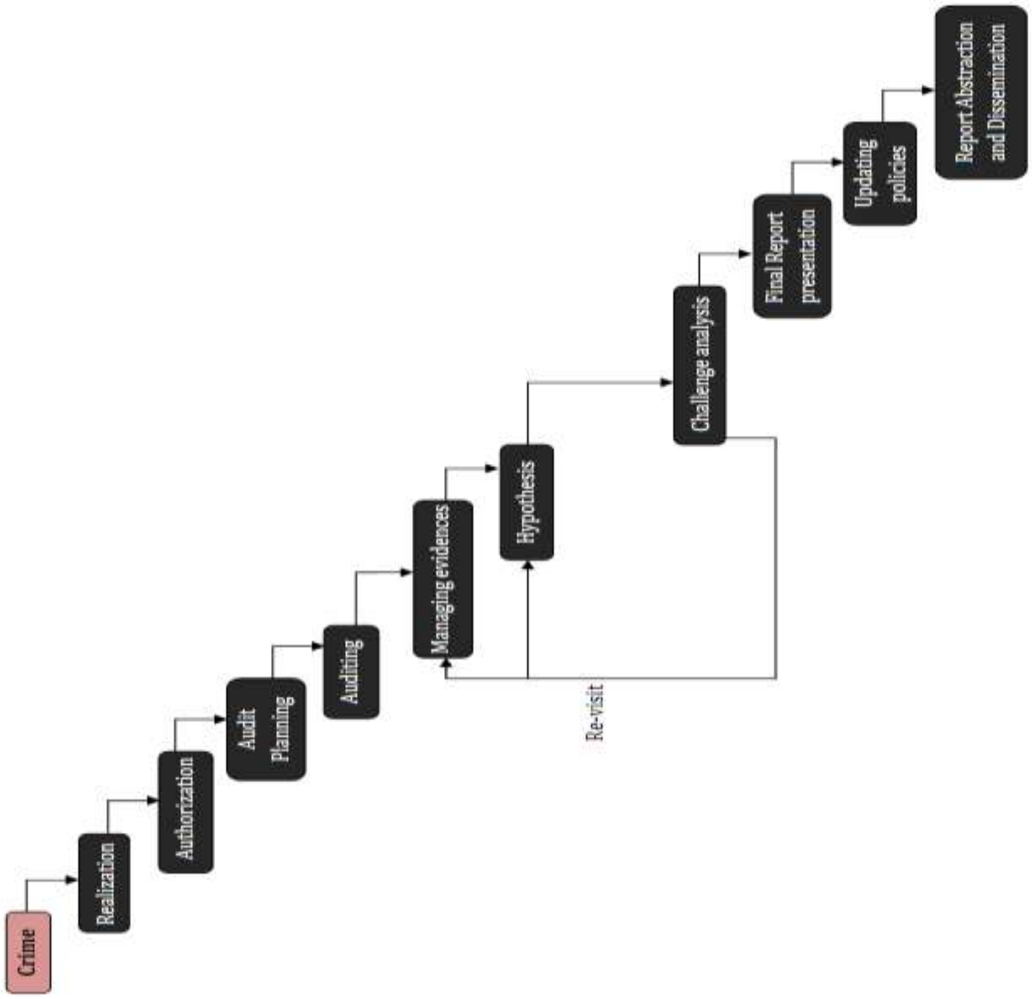
V. PHASES OF CYBER CRIME INVESTIGATION MODEL

A new model for cyber crime investigation has been described here. The inclusion of information flow, as well as the investigative activities, makes it more complete than other models. The proposed model have various phases as: Realization phase, Authorization phase, Audit planning, Auditing, Managing evidence, Hypothesis, Challenge analysis, Final report presentation, Updating polices, Report abstraction and Dissemination.

Each phase has its own importance in the model and is placed in sequence. The sequence goes like this: In realization phase the particular organization/system/individual realizes that some form of cyber crime has occurred. Authorization phase is the mirror to the communication process between the investigating team and the organization/person which is suffering or has suffered from the cyber crime. In audit planning all the necessary preparations are done before reaching the location of crime, by any of the mode or medium. The basic concept behind the auditing is to extract/discover the data and then match/recognize the piece of digital evidence. In Managing evidences phase, the investigating team collects relevant evidences for providing the crime’s effect and to reach the criminal/conclusion. This is the phase in which the investigating team tries to go against their own built hypothesis and try to prove their own hypothesis wrong and irrelevant. The main motto is to prove the validity of the hypothesis and defend it against criticism and challenge. In this phase, a final report of the whole investigation process is generated and presented well in front of the relevant person or organization and the opposition party. In updating policies phase, the security policies of the organization and the standard policies are reconsidered and updated if required with respect to the organizational level and to the standard levels if required. The final activity in the model is the dissemination of information from the investigation.

As cyber crime is transnational in nature, so the proposed model is to be implied after the confirmation of the site, where the actual cyber crime has taken place.

Figure 1.1 Shows the overview of proposed Cyber Crime Investigation Model



VI. CONCLUSION

In this research, a new cyber crime investigation model has been introduced which is structured in nature and has been customized for any type of digital crime .It is user friendly, which tries to capture the full scope of an investigation process .The proposed model focuses more into efficiency, accuracy and how to preserve the fragile evidence, its transport and storage. Main concern for the investigator is on the flow of information of the model and then the audit planning along with auditing of the cyber crime investigation. This model allows technical requirements for each phase to be developed and for the interaction between physical and digital investigations to be identified. It can be used in a practical way to identify opportunities for the development and operation of technology to support the work of investigators. It also provides a framework for the capture and analysis of requirements for investigative tools, particularly for advanced automated analytical tools. It can be used to help develop and apply methodologies to new technologies as they emerge and become the subject of investigations.

REFERENCES

[1]. M.Pollitt, An ad-hoc review of digital forensics models, in Book Chapter from Cybercrime: An Introduction to an Emerging Phenomenon, G.Higgins, Editor, McGraw Hill.

[2]. G.Palmer, A Road Map for Digital Forensic Research: Report from the First Digital Forensic Workshop, in Online: http://www.dfrws.org/dfrws-rm-final.pdf, D.T.R. DTR-T001-01, Editor. 2001.

[3]. M.Reith, C.C., G.Gunsch, An Examination of Digital Forensics Models. International Journal of Digital Evidence, 2002. **1**(3): p. 1-12.

[4]. B.Carrier, E.H.S., Getting Physical with the Investigative Process. International Journal of Digital Evidence, 2003. **2**(2).

[5]. B.Carrier, E.H.S., Getting Physical with the Investigative Process. International Journal of Digital Evidence, 2004. **2**(2).

[6]. Stephenson, P.R., Towards Improving Attribution Confidence in Cyber Attacks. Journal of Cyber conflict studies, 2006. **1**(1): p. 48-53

[7]. V.Baryamureeba, F.T., The Enhanced Digital Investigation Process Model. Digital Forensic Research Workshop, 2004.

[8]. S.O.Ciardhuáin, An Extended Model of Cybercrime Investigation. International Journal of Digital Evidence, 2004. **3**(1).

[9]. N.L.Beebe, J.G.C., A hierarchical, object- based framework for the digital investigation process. Digital Investigation Process Framework, 2004. **2**: p. 147–167.

[10]. Michael Kohn, J.E., Ms Olivier, Framework for Digital Forensic Investigation: Information and Computer Security Architectures Research Group (ICSA), University of Pretoria

[11]. M.K.Rogers, J.G., R.Mislan, T.Wedge, S.Debrota. Computer Forensic Field. Triage Process Model. in International Conference on Digital Forensics, Security and Law. 2006.

[12]. Freiling, B.c. A Common Process Model for Incident Response and Computer Forensics. in Proceedings of Conference on IT Incident Management and IT Forensics. 2007.