Computer Profiling Based Model for Investigation

Neeraj Choudhary
M.Tech Scholar
CS Deptt. PCST Bhopal
neerajpcst@yahoo.com

Nikhil Kumar Singh
Assistant Professor
CS Deptt. PCST Bhopal
nikil30_singh@yahoo.co.in

Parmalik Singh
Assistant Professor
CS Deptt. PCST Bhopal
parmalik83@gmail.com

ABSTRACT
Computer profiling is used for computer forensic analysis, and proposes and elaborates on a novel model for use in computer profiling, the computer profiling object model. The computer profiling object model is an information model which models a computer as objects with various attributes and inter-relationships. These together provide the information necessary for a human investigator or an automated reasoning engine to make judgments as to the probable usage and evidentiary value of a computer system. The computer profiling object model can be implemented so as to support automated analysis to provide an investigator with the information needed to decide whether manual analysis is required.

Keywords
Computer Profiling, User profile, Automated Models, Forensic.

1. INTRODUCTION

There is a need of analysis of computers, its resources and users of computer system for forensic investigation, for digital facts every resource must be examined in a computer for perfect investigation. For doing investigation, manual process takes long time and energy, it is not possible to complete the process with in short spell of time. So investigators can adopt an automated process which is computer profiling or user profiling to conduct a forensic rebuilding of a computer system. By this process, the computer profile, allows an examiner to make a formal decision regarding what are resources which will be examined. Computer profiling or user profiling can be lead to make right investigation. Automated computer profiling facilitates by producing a formal hypotheses of a computer system about the computer system's activity. These hypotheses can be used with successive investigation. In this paper we explain formal models to support automated computer profiling. These formal models the computer profiling object model, can be used as the basis for the practical implementation of computer profiling tools.

2. USER PROFILE

A user profile is a record of personal data linked to a particular user [1]. A profile represents a person on the computer system and it is a logical identity of a person. A user profile can also be considered as the computer representation of a user model. User profile may include private data, files, setting of software, application, and connections which are being used. A profile can be used to keep to the information of a person. This information can be used by systems that personalize the human computer interaction. User's profiles can be found at different level like operating systems, application software or dynamic websites such as social networking web sites [2].

Types of users

There are basically three types of users at different level first is Operating System level users, second is Application level users and last one is Database users.

3. PROFILING FOR FORENSIC

To gather information about the computer and users for forensic analysis and trace a computer model in order to draw a profile. The term forensic means information that is used as proof. In particular, forensic profiling is the process of finding out relations between data in data bases that can be used to identify and represent an offender.

4. PROFILING TECHNIQUES

Profiling is usually carried out using data mining technology, with the help of data mining techniques appropriate information, patterns are automatically discovered, and profiles are generated from large data set.

There are many types of accounts or profiles in the computer system at different level by which investigation can be done.

5. DATA AVAILABLE FOR PROFILING

There are two kinds of data available for user profiling, nominal data and criminal data, nominal data may be obtained from user profile, for investigations, for example a mobile number can be traced and further information can be gather using registration forms, criminal data consist of traces that result from illegal activities, this type of data can be gather by conducting an investigation based on history or previous activities of the uses.

6. PROFILING INVESTIGATION

Which refers to the analysis of resources of computer which may be user profiles, digital data, files, application programs etc. which are used by end users.

7. PROFILING ISSUES

Privacy is a measure concern of the security, the use of profiling for investigation is threats to the privacy of the individual or end users. In reality, criminal data often consists of personal data. One of the critical issues is privacy must not be affected and must not be revealed during criminal investigation. Several issues technical, legal, and behavioral-are available associated with forensic profiling should be considered.

8. REVIEW OF AUTOMATED MODELS FOR FORENSIC ANALYSIS

An automated model use for profiling of a computer system is obviously helpful to the implementation of an automated process to analyze a computer system. In practice, the proper process of investigation employing computational models to check and remove hypotheses, with plenty computational resources, a computer program could potentially represent the complete primitive and complex history of a computer system, and to infer all possible histories of that computer system. It is necessary, however, to narrow the scope of any automated forensic analysis in order to make that analysis computationally feasible. The objective for a model conceived to support computer profiling is slightly different from models conceived to support manual forensic analysis. An automated forensic analysis of a computer system with the intention of providing an investigator an overview of the computer system, its history, and possible areas of interest for further investigation, does not conform to the hypothesis testing approach. Instead, it is intended to help inform the formulation of a hypothesis or several hypotheses about the computer system's history. This sort of automated forensic analysis is computer profiling, the topic of this paper. Practical computer profiling is limited by imperfect records of user and system activity, imperfect understanding of the operation of hardware and software. In this paper just an overview of present automated profiling models.

8.1 THE COMPUTER PROFILING OBJECT MODEL

The computer profiling object model presents a skeleton for the system activities for the purpose of forensic analysis. This approach uses the principles of entity-relationship model for representing a computer system for investigation [3].

8.1.1 Objects

According to this model first we should discovered all the entities on a target machine and assigned an object type, then divide into one of the four categories. Each object type in the object type hierarchy represents an element of the computer system. The four types of object are system objects represent configuration data, and system software, hardware etc. second one is principal objects represent people or groups of people associated with the computer. Subtypes include User objects, Group objects, and Organization objects. Third is application objects represent the programs which have been installed on the computer system, fourth and last is content objects represent data files. Subtypes include Document objects, Image objects, Video objects etc [3].

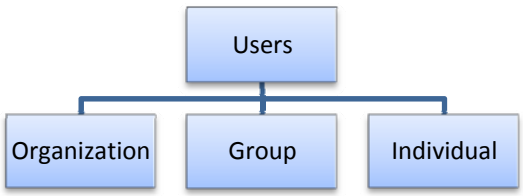

Figure 1

8.1.3 Relationships

The above defined objects may be linked to each other, like represents some relation between objects. Relationships are important element of the computer profile. The relationships between objects is potentially of great advantage to an investigator, if there is a relationships link which is suspect object to other objects, it may be a sources of evidence. A relationship between objects lets an examiner to know an object as a section of evidence in the context of an investigation. For example, an Individual object (object set U), user, might have different accounts (objects) at different level (object set AC), A, D, O. If U is recognized in an investigation as an object, then the relationships can be found between the objects[3], illustrated in Fig. 2.

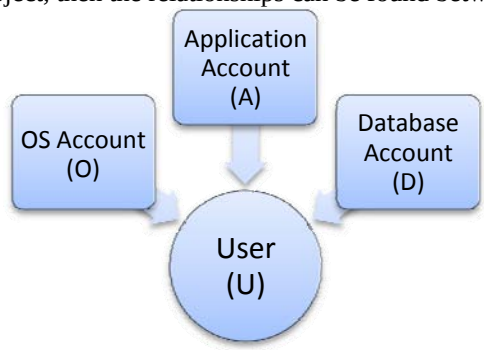

Figure 2

8.2.3 Event and Time

The set of events which occurred in the history forms an important part of the profile computer system. The inclusion of the set of all events in the computer profile allows for the reconstruction of timelines of computer activity. Connecting the events in the history of the computer system with the objects they concern facilitates the tracing of the history of particular objects. This permits selective time-lining, focusing on the object(s) which are of most interest to a digital investigation. Time-lining is an extremely important activity in many digital investigations [3].

9. FUTURE APPROACH

As we mentioned above there are different types of user at different levels. Presently it is possible to login as an OS level user after logging it is possible to access application or database by other user's account. In future work, we will try to make user profile as well as computer profile that will make easer investigation process. We will classify different users at different levels.

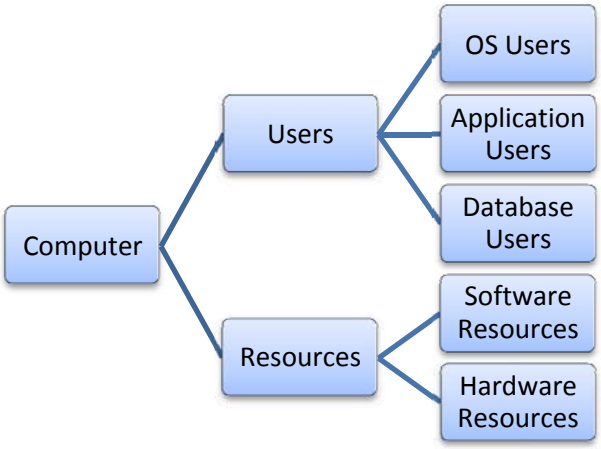

Figure 3

10. CONCLUSION

The computer profiling models present a structure for development of automated computer forensic investigation. The models make possible digital evidence representation, and computer activity for the purpose of investigation. There are different resources in the computer by which investigation process takes place. Computer profiling assists investigators and saves time for making abstract view of the computer. In this paper

we have reviewed previously proposed models; on the ground of this model we have focused on classifying computer's users at different levels. That can make this investigation process easier.

11. ACKNOWLEDGMENT

The research presented in this paper would not have been possible without our college, at ---------, Bhopal. The Authors wish to express our gratitude to all the people who helped turn the World-Wide Web into the useful and popular distributed hypertext it is. We also wish to thank the anonymous reviewers for their valuable suggestions.

REFERENCES

[1] http://en.wikipedia.org
[2] http://searchsecurity.techtarget.com
[3] "A Model for Computer Profiling" International conference in 2010.