Wireless Pers Commun (2011) 56:5–19
DOI 10.1007/s11277-009-9886-x

An Ontology-driven Model for Digital Forensics Investigations of Computer Incidents under the Ubiquitous Computing Environments

Hai-Cheng Chu · Der-Jiunn Deng · Han-Chieh Chao

Published online: 2 December 2009

Abstract Innumerable firms are extensively integrating state-of-the-art ICT to boost the competitiveness of the organizations in all aspects. Simultaneously, the unprecedented availability of UC networks and mobile devices are exponentially growing. Unfortunately, based on the current voluminous computer crime incidents, the ICT deployments under UC infrastructures might jeopardize the organizations if they ignore the imminent necessity of DF in their homogeneous/heterogeneous ISs. Most enterprises are dearth of vigilance concerning the above issues although they might be aware that the salient and stringent computer crimes are capable of devastating the company's intangible assets silently. Vandalism of intellectual property or conducting industrial espionage for the valuable assets via trustworthy UC networks becomes an approaching menace. Hence, the DF plays an essential role in the information security arena. Demonstrably, there is no one DF suite can encompass all aspects or purposes due to the dynamic diversities of computer crimes in their natures. Interchangeably utilizing various DF tools is a decent approach to find the causes for the associate computer crimes and prevents the related information security incidents from occurring. At last, a DF scenario review utilizing the proposed ontology-driven model with respect to the UC environment was conducted and demonstrated.

H.-C. Chu (✉)
Department of Information Management/International Business, Tunghai University, Taichung, Taiwan
e-mail: hcchu@thu.edu.tw

D.-J. Deng
Department of Computer Science and Information Engineering, National Changhua University of Education, Changhua, Taiwan
e-mail: djdeng@cc.ncue.edu.tw

H.-C. Chao
Department of Electronic Engineering, Institute of Computer Science & Information Engineering, National Ilan University, Ilan, Taiwan
e-mail: hcc@niu.edu.tw

H.-C. Chao
Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan

Keywords Ubiquitous computing · Digital forensics · Computer crime · Information security · Ontology-driven model

1 Introduction

As the Ubiquitous Computing (UC) becomes prevalent and dominant, more unscrupulous Internet technology hacktivists commit swindles towards innocent victims via this ever growing technology. As Information Communication Technology (ICT) progresses on a daily basis, many enterprises have utilized homogeneous/heterogeneous Information Systems (ISs) and Applications Programs (APs) into their core operations in order to achieve competitiveness in the related arenas. Indeed, business operation efficiency has been improved due to tremendously huge amount of corporate data being digitalized, transmitted, shared, processed and stored in diverse databases across the Internet. However, due to the vulnerability of ISs or security leakages in the APs under the UC environments, deceitful information predators or crime syndicate exist somewhere in the networks desperately hunting for innocent victims in order to pursuit their criminal and lucrative purposes.

Currently, from desktop PCs to mobile devices are widely utilizing ubiquitous wireless communication infrastructures. MWLAN (Metropolitan Wireless Local Area Network), Wireless Personal Communication (WPC) network, Wi-Fi, 3G, and WiMAX are playing essential roles in Future Communication Computing (FCC). Under such circumstances, information leakage and security threatening have become a seriously challenging issue. An untrustworthy wireless Access Point (AP) may reveal classified or precious intangible assets to hackers, which results in unexpected disaster for individuals or enterprises without any awareness of the current users. Digital Forensics (DF) is a newly emerging research filed, which is different from computer security that is emphasized on the prevention of computer crimes. Digital Forensics is focusing on the digital evidence, which is a digital trail that the suspect intentionally or accidentally left behind on the crime scene and it might be volatile in its nature [1]. Digital Forensics is practiced in both public sector and private sector. For public sector, law enforcement prosecutors play a fundamental role in this field. For private sector, some ISs consulting corporations are capable of providing this kind of service. Undoubtedly, most firms prefer to handle the computer crimes themselves instead of filing to the law enforcement because chain of custody of digital evidences may accidentally reveal company's confidential documents, which the organizations can not afford to take the risk in terms of business profitability.

Generally speaking, the distinct DF stages encompass the procedures of *identification, collection, extraction, preservation* and *interpretation* of the digital evidence that was present concerning a computer incident or confidentiality breach [13]. Once the computer incident occurs, any organization needs to find the causes immediately in order to stop the continuous information security breaches. As we stated above, most corporations are not willing to disclose the security incident to law enforcement due to the fact that the disclosure of the incident might give the chance for their competitors to take advantage of the exploited vulnerability, which may results in recoverable disasters in the market shares. Consequently, DF specialists in the private sector become crucial once the situation occurs. If the DF staff is not capable of capturing the intangible digital trails that the suspect left behind timely or appropriately, the digital evidences could be disappeared, altered or erased by the intruder [7]. In many cases, the digital evidence is unrecoverable. The DF staff is indispensable to unveil the causes of the incident in order to prevent the similar potential computer crimes from occurring or threatening the enterprise. Accordingly, in this research, we proposed an ontology-driven model and guidelines with respect to UC environments for the DF staff to consider and follow if a computer incident occurs.

The scientific contributions of the paper are the proposed ontology-driven model for DF investigations under UC environments, which provided ontological guidelines for the DF staffs to integrate with the investigation topology, which few researches have explored. Additionally, the DF staffs need to utilize the open source software or proprietary toolkits to deal with the obfuscations. We also provided a DF scenario review by adopting some popular DF tools (*ProDiscover Basic AccessData-FTK* and *Guidance Software-EnCase eDiscovery*) integrating with the distinct DF procedures presented in this paper. At last, we carried on DF tools assessment criteria among these software suites based on the key forensics functionalities during the investigation. The assessment criteria of the above tools provide clear guiding principles for the DF staff to ponder. This paper is also attempting to shrink the theory-practice gap in this challenging DF arena.

2 Related Researches Concerning DF

In the past two decades, computer crimes and computer-related crimes have mushroomed in all countries because networks become ubiquitous. Generally speaking, the computer crime means the computers become the target of cyber attacks, such as denial of service attacks or virus attacks. The computer-related crime stands for the use of computers storage devices and ICT tools to commit cybercrimes, such as corporate frauds [4,14]. For most computer crackers, they may accidentally leave some kind of digital trails, which represent digital evidences that can be used to prosecute the criminals in a court of law in order to hinder these ever growing high-tech crimes that resulted in tremendous financial losses worldwide [6].

The DF emerges and becomes the critical factor to prosecute the culprit by law enforcement and prevents the associate cybercrime incidents from recurring in the public sector. Unfortunately, very few colleges/universities programs worldwide offer a comprehensive curriculum that encompasses this appearing knowledge as well as the skill sets [2,10,17]. Basically, DF and Computer Forensics are used interchangeably in the research literatures. Due to voluminous literatures on the problem of computer crimes, there is an urgent necessity for the DF specialists in both public and private sectors.

Obviously, the DF is still in its infant stage and possesses a pressing need for direction and definition for colleges/universities to establish the associate certifications or curriculum programs as well as pedagogical models. The ICT-savvy hacktivists are committing heinous swindles on the Internet. Hence, the forensics science community has become aware of the importance of DF and it must be addressed as a professional and a science, which will be closely related to many court cases in the public sector [16]. The DF is consisted of a multidisciplinary curriculum, which is based on the disciplines of criminology and profound ICT knowledge. Researches pointed out that the essential DF category includes crime, computer, security, legislation, investigation processes and forensics tools. Based on existing researches, generally speaking, the DF is a serial investigation procedure of information security threat where there is a digital evidence for the suspicious behavior regarding the sinister side of computer manipulation. It encompasses the stages of *Planning, Identification, Collection, Classification, Preservation, Analysis, Reconstruction, Documentation, and Presentation* of electronic evidences in a legitimate manner to investigate the suspect to be inculpatory or exculpatory in a court of law in the public sector or terminate an employee for his/her policy violation concerning computer usage in the private sector. In this paper, we conducted the following concise categories without losing the spirit of the detailed stages to go through