Xuejia Lai
Dawu Gu
Bo Jin
Yongquan Wang
Hui Li (Eds.)

LNICST 56

Forensics in Telecommunications, Information, and Multimedia

LNICST

Third International ICST Conference, e-Forensics 2010
Shanghai, China, November 2010
Revised Selected Papers

ICST

Springer

Lecture Notes of the Institute
for Computer Sciences, Social Informatics
and Telecommunications Engineering 56

Xuejia Lai Dawu Gu Bo Jin
Yongquan Wang Hui Li (Eds.)

Forensics in Telecommunications, Information, and Multimedia

Third International ICST Conference,
e-Forensics 2010
Shanghai, China, November 11-12, 2010
Revised Selected Papers

Springer

Volume Editors

Xuejia Lai
Dawu Gu
Shanghai Jiao Tong University, Department of Computer
Science and Engineering, 200240 Shanghai, P.R. China
E-mail: lai-xj@cs.sjtu.edu.cn; dwgu@sjtu.edu.cn

Bo Jin
The 3rd Research Institute of Ministry of Public Security
Zhang Jiang, Pu Dong, 210031 Shanghai, P.R. China
E-mail: jinbo@stars.org.cn

Yongquan Wang
East China University of Political Science and Law
Shanghai 201620, P. R. China
E-mail: wangyquan@sina.com

Hui Li
Xidian University Xi'an, Shaanxi 710071, P.R. China
E-mail: xd.lihui@gmail.com

ISSN 1867-8211
ISBN 978-3-642-23601-3
DOI 10.1007/978-3-642-23602-0

e-ISSN 1867-822X
e-ISBN 978-3-642-23602-0

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011935336

CR Subject Classification (1998): C.2, K.6.5, D.4.6, I.5, K.4, K.5

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

E-Forensics 2010, the Third International ICST Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia, was held in Shanghai, China, November 11-12, 2010. The conference was sponsored by ICST in cooperation with Shanghai Jiao Tong University (SJTU), the Natural Science Foundation of China (NSFC), Science and Technology Commission of Shanghai Municipality, Special Funds for International Academic Conferences of Shanghai Jiao Tong University, the 3rd Research Institute of the Ministry of Public Security, China, East China University of Political Science and Law, China, NetInfo Security Press and Xiamen Meiya Pico Information Co. Ltd.

The aim of E-Forensics conferences is to provide a platform for the exchange of advances in areas involving forensics such as digital evidence handling, data carving, records tracing, device forensics, data tamper identification, mobile device locating, etc. The first E-Forensics conference, E-Forensics 2008, was held in Adelaide, Australia, January 21–22, 2008; the second, E-Forensics 2009, was held in Adelaide, Australia, January 19–21, 2009.

This year, the conference received 42 submissions and the Program Committee selected 32 papers after a thorough reviewing process, appear in this volume, together with 5 papers from the Workshop of E-Forensics Law held during the conference. Selected papers are recommended for publication in the journal *China Communications*.

In addition to the regular papers included in this volume, the conference also featured three keynote speeches: "Intelligent Pattern Recognition and Applications" by Patrick S. P. Wang of Northeastern University, USA, "Review on Status of Digital Forensic in China" by Rongsheng Xu of the Chinese Academy of Sciences, China, and "Interdisciplinary Dialogues and the Evolution of Law to Address Cybercrime Issues in the Exciting Age of Information and Communication Technology" by Pauline C. Reich of Waseda University School of Law, Japan.

The TPC decided to give the Best Paper Award to Xiaodong Lin, Chenxi Zhang, and Theodora Dule for their paper "On Achieving Encrypted File Recovery" and the Best Student Paper Award to Juanru Li, Dawu Gu, Chaoguo Deng, and Yuhao Luo for their paper "Digital Forensic Analysis on Runtime Instruction Flow."

Here, we want to thank all the people who contributed to this conference. First, all the authors who submitted their work; the TPC members and their external reviewers, the organizing team from the Department of Computer Science and Engineering of Shanghai Jiao Tong University—Zhihua Su, Ning Ding,

Jianjie Zhao, Zhiqiang Liu, Shijin Ge, Haining Lu, Huaihua Gu, Bin Long, Kai Yuan, Ya Liu, Qian Zhang, Bailan Li, Cheng Lu, Yuhao Luo, Yinqi Tang, Ming Sun, Wei Cheng, Xinyuan Deng, Bo Qu, Feifei Liu, and Xiaohui Li—for their great efforts in making the conference run smoothly.

November 2010

Xuejia Lai
Dawu Gu
Bo Jin
Yongquan Wang
Hui Li

Organization

Steering Committee Chair

Imrich Chlamtac	President Create-Net Research Consortium

General Chairs

Dawu Gu	Shanghai Jiao Tong University, China
Hui Li	Xidian University, China

Technical Program Chair

Xuejia Lai	Shanghai Jiao Tong University, China

Technical Program Committee

Xuejia Lai	Shanghai Jiao Tong University, China
Barry Blundell	South Australia Police, Australia
Roberto Caldelli	University of Florence, Italy
Kefei Chen	Shanghai Jiao Tong University, China
Thomas Chen	Swansea University, UK
Liping Ding	Institute of Software, Chinese Academy of Sciences, China
Jordi Forne	Technical University of Catalonia, Spain
Zeno Geradts	The Netherlands Forensic Institute, The Netherlands
Pavel Gladyshev	University College Dublin, Ireland
Raymond Hsieh	California University of Pennsylvania, USA
Jiwu Huang	Sun Yat-Sen University, China
Bo Jin	The 3rd Research Institute of the Ministry of Public Security, China
Tai-hoon	Kim Hannam University, Korea
Richard Leary	Forensic Pathway, UK
Hui Li	Xidian University, China
Xuelong Li	University of London, UK
Jeng-Shyang	Pan National Kaohsiung University of Applied Sciences, Taiwan
Damien Sauveron	University of Limoges, France
Peter Stephenson	Norwich University, USA
Javier Garcia	Villalba Complutense University of Madrid, Spain

Jun Wang	China Information Technology Security Evaluation Center
Yongquan Wang	East China University of Political Science and Law, China
Che-Yen Wen	Central Police University, Taiwan
Svein Y. Willassen	Norwegian University of Science and Technology, Norway
Weiqi Yan	Queen's University Belfast, UK
Jianying Zhou	Institute for Infocomm Research, Singapore
Yanli Ren	Shanghai University, China

Workshop Chair

Bo Jin	The 3rd Research Institute of the Ministry of Public Security, China
Yongquan Wang	East China University of Political Science and Law, China

Publicity Chair

Liping Ding	Institute of Software, Chinese Academy of Sciences, China
Avinash Srinivasan	Bloomsburg University, USA
Jun Han	Fudan University, China

Demo and Exhibit Chairs

Hong Su	NetInfo Security Press, China

Local Chair

Ning Ding	Shanghai Jiao Tong University, China

Publicity Chair

Yuanyuan Zhang	East China Normal University, China
Jianjie Zhao	Shanghai Jiao Tong University, China

Web Chair

Zhiqiang Liu	Shanghai Jiao Tong University, China

Conference Coordinator

Tarja Ryynanen	ICST

Workshop Chairs

Bo Jin	The 3rd Research Institute of the Ministry of Public Security, China
Yongquan Wang	East China University of Political Science and Law, China

Workshop Program Committee

Anthony Reyes	Access Data Corporation, Polytechnic University, USA
Pauline C. Reich	Waseda University, Japan
Pinxin Liu	Renmin University of China, China
Jiang Du	Chongqing University of Posts and Telecommunications, China
Denis Edgar-Nevill	Canterbury Christ Church University, UK
Yonghao Mai	Hubei University of Police, China
Paul Reedy	Manager Forensic Operations Forensic and Data Centres, Australia
Shaopei Shi	Institute of Forensic Science, Ministry of Justice, China
Man Qi	Canterbury Christ Church University, UK
Xufeng Wang	Hangzhou Police Bureau, China
Lin Mei	The 3rd Research Institute of the Ministry of Public Security, China

Table of Contents

On Achieving Encrypted File Recovery

Xiaodong Lin[1], Chenxi Zhang[2], and Theodora Dule[1]

[1] University of Ontario Institute of Technology, Oshawa, Ontario, Canada
{Xiaodong.Lin,Theodora.Dule}@uoit.ca
[2] University of Waterloo, Waterloo, Ontario, Canada
c14zhang@engmail.uwaterloo.ca

Abstract. As digital devices become more prevalent in our society, evidence relating to crimes will be more frequently found on digital devices. Computer forensics is becoming a vital tool required by law enforcement for providing data recovery of key evidence. File carving is a powerful approach for recovering data especially when file system metadata information is unavailable. Many file carving approaches have been proposed, but cannot directly apply to encrypted file recovery. In this paper, we first identify the problem of encrypted file recovery, and then propose an effective method for encrypted file recovery through recognizing the encryption algorithm and mode in use. We classify encryption modes into two categories. For each category, we introduce a corresponding mechanism for file recovery, and also propose an algorithm to recognize the encryption algorithm and mode. Finally, we theoretically analyze the accuracy rate of recognizing an entire encrypted file in terms of file types.

Keywords: Data Recovery, File Carving, Computer Forensics, Security, Block Cipher Encryption/Decryption.

1 Introduction

Digital devices such as cellular phones, PDAs, laptops, desktops and a myriad of data storage devices pervade many aspects of life in today's society. The digitization of data and its resultant ease of storage, retrieval and distribution have revolutionized our lives in many ways and led to a steady decline in the use of traditional print mediums. The publishing industry, for example, has struggled to reinvent itself by moving to online publishing in the face of shrinking demand for print media. Today, financial institutions, hospitals, government agencies, businesses, the news media and even criminal organizations could not function without access to the huge volumes of digital information stored on digital devices.

Unfortunately, the digital age has also given rise to digital crime where criminals use digital devices in the commission of unlawful activities like hacking, identity theft, embezzlement, child pornography, theft of trade secrets, etc. Increasingly, digital devices like computers, cell phones, cameras, etc. are found at crime scenes during a criminal investigation. Consequently, there is a growing need for investigators to search digital devices for data evidence including

X. Lai et al. (Eds.): E-Forensics 2010, LNICST 56, pp. 1–13, 2011.

emails, photos, video, text messages, transaction log files, etc. that can assist in the reconstruction of a crime and identification of the perpetrator. One of the decade's most fascinating criminal trials against corporate giant Enron was successful largely due to the digital evidence in the form of over 200,000 emails and office documents recovered from computers at their offices. Digital forensics or computer forensics is an increasingly vital part of law enforcement investigations and is also useful in the private sector for disaster recovery plans for commercial entities that rely heavily on digital data, where data recovery plays an important role in the computer forensics field.

Traditional data recovery methods make use of file system structure on storage devices to rebuild the device's contents and regain access to the data. These traditional recovery methods become ineffective when the file system structure is corrupted or damaged, a task easily accomplished by a savvy criminal or disgruntled employee. A more sophisticated data recovery solution which does not rely on the file system structure is therefore necessary. These new and sophisticated solutions are collectively known as file carving. File carving is a branch of digital forensics that reconstructs data from a digital device without any prior knowledge of the data structures, sizes, content or type located on the storage medium. In other words, the technique of recovering files from a block of binary data without using information from the file system structure or other file metadata on the storage device.

Carving out deleted files using only the file structure and content could be very promising [3] due to the fact that some files have very unique structures which can help to determine a file's footer as well as help to correct and verify a recovered file, e.g., using a cyclic redundancy check (CRC) or polynomial code checksum. Recovering contiguous files is a trivial task. However, when a file is fragmented, data about the file structure is not as reliable. In these cases, the file content becomes a much more important factor than the file structure for file carving. The file contents can help us to collect the features of a file type, which is useful for file fragment classification. Many approaches [4,5,6,7,8] of classification for file recovery have been reported and are efficient and effective. McDaniel et al. [4] proposed algorithms to produce file fingerprints of file types. The file fingerprints are created based on byte frequency distribution (BFD) and byte frequency cross-correlation (BFC). Subsequently, Wang et al. [5] created a set of modes for each file type in order to improve the technique of creating file fingerprint and thus to enhance the recognition accuracy rate: 100% accuracy for some file types and 77% accuracy for JPEG file. Karresand et al. [7,8] introduced a classification approach based on individual clusters instead of entire files. They used the rate of change (RoC) as a feature, which can recognize JPEG file with the accuracy up to 99%.

Although these classification approaches are efficient, they have no effect on encrypted files. For reasons of confidentiality, in some situations, people encrypt their private files and then store them on the hard disk. The content of encrypted files is a random bit stream, which provides no clue about original file features or useful information for creating file fingerprints. Thus, traditional classification

approaches cannot be directly applied to encrypted file recovery. In this paper, we introduce a recovering mechanism for encrypted files. To the best of our knowledge, this is the first study of encrypted file recovery. Firstly, we categorize block cipher encryption mode into two groups: block-decryption-dependant, and block-decryption-independent. For each group, we present an approach for file recovery. Secondly, we present an approach for recognizing block cipher mode and encryption algorithm. Based on the introduced approach, encrypted files can be recovered. Lastly, we analyze our proposed scheme theoretically.

The rest of the paper is organized as follows. Section 2 briefly introduces problem statement, objective and preliminaries that include file system, file fragmentation, and file encryption/decryption. According to different block cipher encryption modes, Section 3 presents a corresponding mechanism for file recovering. Section 4 introduces an approach of recognizing a block cipher mode and an encryption algorithm. Section 5 theoretically analyzes our proposed approach. Finally, we draw the conclusions of this study and give the future work in Section 6.

2 Preliminaries and Objective

2.1 File System and File Fragmentation

We use the FAT file system as an example to introduce general concepts about file systems. In a file system, a file is organized into two main parts: (1) The first part is the file identification and metadata information, which tell an operating system (OS) where a file is physically stored; (2) The second part of a file is its physical contents that are stored in a disk data area. In a file system, a cluster (or block) is the smallest data unit of transfer between the OS and disk. The name and starting cluster of a file is stored in a directory entry, which presents the first cluster of the file. Each entry of a file allocation table (FAT) records its next cluster number where a file is stored and a special value is used to indicate the end of file (EOF), for example, 0xffffffff as end of cluster chain markers for one of three versions of FAT, i.e., FAT32. As shown in Fig. 1, the first cluster number of file a.txt is 32, and the following cluster number is 33, 39, 40. When a file is deleted, its corresponding entries at the file allocation table are wiped out to zero. As shown in Fig. 1, if a.txt is deleted, the entries, 32, 33, 39, and 40, are set to "0". However, the contents of a.txt in the disk data area remain. The objective of a file carver is to recover a file without the file allocation table.

When files are first created, they may be allocated in disk entirely and without fragmentation. As files are modified, deleted, and created over time, it is highly possible that some files become fragmented. As shown in Fig. 1, a.txt and b.txt are fragmented, and each of them are fragmented into two fragments.

2.2 Problem Statement and Objective

We will now give an example to properly demonstrate the issue we will address in this paper. Suppose that there are several files in a folder. Some files are