COMPREHENSIVE ANALYSIS ON HARDWARE FORENSIC FOR GAMBLING MACHINE

PRITHEEGA A/P MAGALINGAM

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Masters of Computer Science (Information Security)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

NOVEMBER 2008

ABSTRACT

Hardware forensic analysis involves process of analyzing digital evidence derived from digital sources in order to facilitate and prove either the device is used to commit crime, contains evidence of crime or it is a target of crime. The digital evidence is analyzed to determine the type of information that is stored. For this purpose special tools might be needed to translate the digital information in a format that is useful to the investigators. Besides other electronic devices that commonly encountered in crime scenes such as computer systems, access control devices, answering machines, personal digital assistants, modems, network components, pagers and etc. which can produce digital evidence, law enforcement also shows their wide concern towards gambling machine which is the main source of conducting illegal game. An illegal game is defined by the law as a game which a player can win money or gifts by the game results and the results is based on chances. Law forbids conducting or involving in such games. This project presents information retrieval method from a gaming machine which was seized and analysis on the information interpreted to prove that the gaming machine is used illegally. These procedures were required by PDRM which will be part of gambling machine forensic process and it will assist them in digital forensic evidence analysis as a guideline to produce evidence which is relevant to prove the illegal gambling.

ABSTRAK

Analisis forensik perkakasan melibatkan proses menganalisa bukti yang diperolehi secara elektronik untuk menunjukkan bukti sama ada peralatan elektronik adalah digunakan untuk melakukan jenayah, mengandungi bukti jenayah atau ia adalah satu sasaran jenayah. Bukti digital dianalisis untuk menentukan jenis maklumat yang disimpan. Bagi tujuan ini, alat yang khas mungkin diperlukan untuk memaparkan maklumat digital dalam satu format yang berguna dan boleh difahami oleh penyiasat. Selain peranti elektronik lain yang biasa ditemui semasa siasatan jenayah seperti sistem komputer, alat kawalan akses, mesin menjawab elektronik, pembantu digital peribadi, modem, komponen jaringan, pagers dan seumpamanya yang mengandungi bukti digital, penguatkuasa undang-undang juga memfokus secara luas ke arah penyalahgunaan mesin permainan yang merupakan sumber utama untuk menjalankan permainan haram. Permainan haram ditakrifkan di sisi undang-undang sebagai suatu perjudian yang membolehkan pemain memenangi hadiah dalam bentuk wang atau produk melalui mata yang dimenangi dalam satu set permainan dan kemenangan tersebut adalah berasaskan peluang. Undang-undang melarang sesiapa yang menjalankan atau melibatkan diri dalam permainan seumpama ini. Objektif utama projek ini adalah untuk memperkenalkan kaedah mendapatkan maklumat dari satu mesin permainan yang telah dirampas dan menganalisis maklumat yang diterjemahkan untuk membuktikan bahawa mesin permainan tersebut digunakan secara haram. Prosedur mendapatkan bukti digital ini dibina atas permintaan PDRM yang akan menggunakan kaedah ini sebagai sebahagian daripada proses forensik mesin perjudian. Kaedah ini akan membantu mereka dalam penganalisaan maklumat digital dan ia boleh dijadikan sebagai satu garis panduan untuk mengenalpasti bukti yang relevan untuk menunjukan aktiviti perjudian haram dijalankan.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Mainstay of crime groups in our country today is due to illegal gambling which has become major challenge to PDRM in the task of eliminating unlawful gambling by providing evidence to court to prove that an owned gaming machine is a gambling machine. Compared to earlier mechanical devices, the current gambling machine is installed with sophisticated computer software and hardware. Locating relevant digital evidence to be a technical prove becomes a difficult task thus the unit needs a proper handling and processing by a forensic expert which will able to avoid problems that could jeopardize the admissibility of evidence. Producing such evidence to court needs detail analyze on the parts of gaming machine hardware which stores data and program, method of extracting data from non-volatile memory and examination of data to find reliable evidence. This project analyze types of method involve in retrieving information from gaming machine memory and propose the evidence acquisition procedure.

1.1.1 Understanding the machine

The gaming machine is build with motherboard which is programmed to provide dual functions allowing the players to use the device for amusement or gambling games. Switching machine mode is common among players to avoid the police to discover of illegal gambling [2]. The structure of the gaming machine

includes a display unit that will generate video images, a value input device, a controller comprising a processor, a random access memory and a non-volatile EPROM (erasable Programmable Read Only Memory) chip. The EPROM is the core of a machine which controls the major activities of the machine [2]. Old machines which are sold are turned into amusement-only machine with new EPROM. If the EPROM used is programmed for gambling, then the device operates illegally.

1.1.2 EPROM chip in gambling machine

Examination on gambling machine electronic board or microcontroller can extract data and program installed in the chips which enable the examiner to identify the operating characteristic of a gambling machine. The EPROM chip has operating system software installed [3]. The functions of EPROM in a gaming machine will be discussed in detail in literature review.

1.1.3 Facts to be proven

Evidence to be produced must support certain facts to prove that a gaming machine is an illegal gambling machine. The location where the prove resides should be identified. EPROM chip which is embedded in the gaming machine microcontroller provides the most because it is the gaming machine's memory and the memory content will not be erased even when the power is plugged off. Following each step in evidence life cycle is essential in order to maintain the integrity of the facts.

1.2 Problem Background

Polis Diraja Malaysia, PDRM experiences severe resource difficulties and doesn't have comprehensive way to provide evidence to court in order to prove that a certain gaming device is a gambling machine. PDRM is responsible for identifying gambling equipment and supplying expert testimonies to court considering the act of crime; illegal gambling.

In order to ensure the evidence provided is strong and admissible in court, there are a number of important analysis steps and guideline should be followed in computer forensic. Proper investigation on illegal gaming machine and analysis of digital evidence covering identification, examination, preservation and presentment of relevant electronic evidence to court is needed to assist PDRM to prevent illegal gambling.

1.3 Problem Statement

PDRM doesn't have sufficient resources and information retrieval method from a gaming machine to provide to court with evidence to prove that a gaming machine is an illegal gambling machine.

1.4 Project Aim

The aim of this project is to develop a digital forensic evidence analysis guideline for a gambling machine and a procedure to translate the retrieved data from gaming machine microprocessor into human readable form for the purpose of providing strong evidence in order to prove illegal gambling activities to the court of law.

1.5 Project Objective

The objectives of the project are as follows:

(a) To design an appropriate method of extracting information from gaming machine.
(b) To ensure the information retrieved can be read and understood by PDRM through a procedure to translate the low level data into human readable form.
(c) To provide a digital forensic evidence analysis guideline for an illegal gambling machine to assist PDRM in the information retrieval process.

1.6 Project Scope

The scope of the project is as follows:

(a) Analyze the chips in gaming machine microprocessor which has the evidential value to prove the machine is used for illegal gambling.
(b) Assumed that the chip in microprocessor is not encrypted and the test will be done on the non-encrypted EPROM. Type of EPROM that will be focused during the implementation phase will be NM27C256Q.
(c) The structure of data should be in low level data form and analysis is conducted on these types of data.
(d) The chip extracting method applies to non-soldered chip on the microcontroller board.

1.7 Project Work Breakdown Structure

Project 1 is estimated to be accomplished within 3 months starting from 4th January 2008 until 7th April 2008 and Project 2 is planned to be accomplished in 6 months from May until October. Project Gantt chart is attached in **Appendix A**.

1.8 Summary

This project contributes to build a digital forensic evidence analysis guideline for a gambling machine and a procedure to interpret the data read from gaming machine microprocessor into a human readable form. Proper analysis has been done in order to ensure its evidentiary value.

REFERENCES

1. SCI Counsel James F. Villere. (1991). Illegal Gambling. Unpublished Report, Division of Criminal Justice in the Attorney General's Department of Law and Public Safety.

2. Steven G.Lemay, Andrew M.Rodges, Robert E.Breckner, Xuedong Chen (2006). EPROM file system in gaming apparatus, structure of a gaming system. *United States Patent No. 7108605*. Retrieved on January 25 2008, from http://www.freepatentsonline.com/7108605.html.

3. Marcel breeuwsma, Martien de Jongh, Coert Klaver, Ronald van der Knijff and Mark Roeloffs. (2007). Forensic Data Recovery From Flash Memory. *Small Scale Digital Device Forensics Journal,* Vol.1, (1). Purdue University.

5. Brian D. Carrier, Joe Grand. (2004). A Hardware-Based Memory Acquisition Procedure for Digital Investigations. *Digital Investigation Journal,* Vol.1, (1). ISSN International Centre.

6. Matthew N. O. Sadiku, Clarence N. Obiozor. Evolution of Computer Systems. Unpublished Report, Temple University, University of North Florida.

7. Kanellis, Kiountouzis, Kolokotronis, Martakos. *Digital Crime and Forensic Science*. Hershey, PA, USA. : Idea Group Inc. 2006.

8. Dr. John L. McMullan, Dr. David C. Perrier. Cheats At Play: The Social Organization Of Video Lottery Terminal Fraud. *Paper presented at the Gambling, Law Enforcement and Justice System Conference*, March Alberta Gaming Institute and University of Alberta: Edmonton, Alberta. 2002.

9. Adam Levinthal and Michael Barnett. (1997) Silicon Gaming Odyssey Slot Machine. *Proceedings of the 42nd IEEE International Computer Conference*. IEEE Computer Society Washington, DC, USA.

10. The National Standard Working Party. (2007). Revision 9.0. Australian /New Zealand Gaming Machine National Standard. New Zealand: Australian and New Zealand gaming regulators.

11. Dr.Elazar (Azi) Zadok, Brig. Gen. Director, D.I.F.S. Gambling Machines Laboratory, Division of Identification and Forensic Science. Unpublished note, Investigation Department/ Israel Police Headquarters.

12. Electronic Engineering Tools, INC. ChipMax Device Programmer. Retrieved on February 20 2008, from http://www.eetools.com.

13. SGS-THOMSON Microelectronic. (1996). 512K(64KX8) UV EPROM and OTP EPROM – M27C512. Retrieved on March 12 2008. http://www.electronicaestudio.com.

14. National Semiconductor. (1989). 262, 144-Bit (32,768 X 8) UV Erasable CMOS PROM – NS27C256. Retrieved on March 12 2008. http://eshop.engineering.uiowa.edu.

15. Don Lancaster and Synergetics.(1985). Programming an EPROM Random number generator.*Ask The Guru*.

16. Memon Asim. Reverse Engineering. Unpublished note, Blekinge Institute of Technology.

17. John Catsoulis. (2005). *Designing Embedded Hardware*. (2nd ed.) USA: O'Reilly.

18. Ryan Leigland, Axel W. Krings. (2004). A Formalization of Digital Forensics. *International Journal of Digital Evidence*, Vol.3, (2). IDJE.

19. Marcel Breeuwsma, Martin De Jongh, Coert Klaver, Ronald van der Knijff and Mark Roeloffs. (2007). Forensic Data Recovery from Flash Memory. *Small Scale Device Forensic Journal*. Vol.1,(1).SSDDFJ.

20. Brian D. Carrier, Joe Grand. (2004). A Hardware-Based Memory Acquisition Procedure for Digital Investigations. *Digital Investigation Journal*. Vol.1, (1). IDJE.

21. Nick L. Petroni, Jr. , AAron Walters, Timothy Fraser, William A. Arbaugh. (2006). FATKit: A Framework for the Extraction and Analysis of Digital Forensic Data from Volatile System Memory. *Digital Investigation Journal*. Vol. 3, (4).

22. Walter R. Siekiersi, Michael Sterling (1985). Random Number Generating Techniques and Gaming Equipment Employing such Techniques. *United States Patent No. 4527798*. Retrieved on July 11 2008, from http://www.freepatentsonline.com/4527798.html.

23. Jean-Michel FRIEDT (2001). *Introduction to the Z84 (Z80 based microcontroller).* Unpublished note, Toshiba (TM-Z84C015).

24. Z8400, SGS. Z80 CPU Central Processing Unit, Product Specification. Retrieved on August 15 2008, from http://www.z80.info/.

25. Barry B. Brey. *The Z80 Microprocessor Hardware, Software, Programming, and Interfacing*. Englewood Cliffs, N.J.: Prentice-Hall,Inc.1988.

26. Muhammad Ali Mazidi, Janice Gillispie Mazidi, Rolin D. Mckinlay. *The 8051 Microcontroller and Embedded Systems Using Assembly and C*. 2nd. ed. Upper Saddle River, N.J.: Pearson Education,Inc.2006.

27. Gaming Labs Certified. (2007). Standard Series. Version 2.0. Client-Server Systems. Gaming Laboratories International, Inc.

28. Michael J. Dietz,II, Earl D. Morris, Rolen A.Miller (1999). Instant, Multiple Play Gaming Ticket And Validation System. *United States Patent No. 5949042*. Retrieved on August 25 2008, from http://www.freepatentsonline.com/5949042.html.

29. John Manship, Michael Vinneau, David Ross, Nathalie Hache, Charles Maillet (1995). Video Gaming Machine. *United States Patent No. 5393061*. Retrieved on September 11 2008, from http://www.freepatentsonline.com/5393061.html.

30. Casino Gambling Terms and Definitions. Retrieved on September 4 2008, from http://www.bestukcasinos.co.uk/casino-terms.html.

31. Dr Benjamin Turnbull. (2008). Forensic Investigation of the Nintendo Wii: A First Glance. *Small Scale Digital Device Forensics Journal,* Vol.2, (1). ISSN.

32. eeTools, EPROM Programmer. Retrieved on March 20 2008, from http://www.eetools.com/index.cfm?fuseaction=devices.do_search.

33. Bingo 8 Line. Retrieved on September 11 2008, from http://www.starlitegaming.com/files/NEW_BINGO_8_LINE.pdf.

34. Kazuyoshi Ishibashi (1996). Display Apparatus For Gaming Machine. *United States Patent No. 5547192*. Retrieved on September 11 2008, from http://www.freepatentsonline.com/5547192.html.