Back to CFET 2008 Index

CFET 2008

2nd International Conference on Cybercrime Forensics Education & Training

Conference Programme & Abstracts

Canterbury Christ Church University
Faculty of Social & Applied Sciences
Department of Computing
North Holmes Road Campus
Powell Building
6th & 7th September 2007

ISBN 1899253-19x

Contents

Introduction to the Conference

Cybercrime Forensics one of the fastest areas of growth within the Computing discipline as it mirrors the explosive growth of criminal activity involving computers. The growing complexity and vulnerability of computer systems and the new forms of criminal activities require research and development to continue to ensure the integrity and security for computer users. The demand for people qualified to assist in cybercrime investigations is very large and growing.

This conference invited papers and presentations on the following:

- Development of cybercrime forensics as a new discipline
- Commercial training in cybercrime forensics
- Supporting police investigations
- Defining educational programmes and their objectives
- Ethical, Professional and legal issues
- New software tools for cybercrime forensics
- International cooperation to develop standards
- Career pathways in cybercrime forensics
- Network and mobile communication technologies
- Cooperation of commercial and academic partners
- Case studies in cybercrime forensics
- Risk management and disaster planning
- Future trends in cybercrime forensics

The conference has attracted a range of speakers, sponsors and delegates from eleven countries. These include serving police officers, high tech crime practitioners, independent consultants, police trainers and university teachers and researchers.

The conference is very grateful to the support provided by its sponsors and the advice and help of the CFET International Advisory Panel (detailed later in this booklet).

I would like to welcome everyone to Canterbury Christ Church University and the Department of Computing who are playing host to this second annual international conference and hope your stay with us is a very enjoyable and informative one.

Denis Edgar-Nevill
Chair, CFET 2008

Conference Venue

The Powell Building was opened in 1999 and named after film maker Michael Powell. Powell's contribution to British, and indeed, to world cinema cannot be overestimated. His influence can be seen in the works of many of today's leading film makers, including Martin Scorsese and Francis Ford Coppola.

Conference Organisers

Conference Chair

Denis Edgar-Nevill Canterbury Christ Church University

Conference Organising Committee

Brian Brighouse Canterbury Christ Church University
Dr Abhaya Induruwa Canterbury Christ Church University
Dr Man Qi Canterbury Christ Church University
Paul Stephens Canterbury Christ Church University
Matthew Tubby Canterbury Christ Church University

International Advisory Panel

Susan Ballou Program Manager, Office of Law Enforcement Standards, NIST, USA

Dr Robin Bryant Head of Crime & Policing, Canterbury Christ Church University, UK

Dr. Joe Carthy University College Dublin, Republic of Ireland

Professor Peter Cooper Department Chair Computer Science, Sam Huston State University, Texas, USA

Dr Philip Craiger Assistant Director for Digital Evidence, National Center for Forensic Science University of Central Florida, USA

Bill Crane Head of Operations, National Digital Crime Investigations Unit, New Zealand

Dr. Rob D'Ovidio Drexel University, USA

Denis Edgar-Nevill Head of Computing, Canterbury Christ Church University, UK

Keerthi Goonatillake School of Computing, University of Colombo, Sri Lanka

Dr Douglas Harris CyberSecurity and Emergency Preparedness Institute, Associate Dean, Erik Jonsson School, Engineering and Computer Science, University of Texas at Dallas, USA

Ron Jewell Manager, Forensic Science Center, Marshall University, USA

Nigel Jones Managing Director, Technology Risk Ltd, UK

Dr Manolya Kavakli Department of Computing, Macquarie University, Australia

Gary C. Kessler Director Center for Digital Investigation Info.Security, Champlain College, USA

Jack McGee President, Justice Institute of British Columbia, Canada

Rob Risen Police Academy of the Netherlands

Professor Sujeet Shonoi University of Tulsa, USA

Professor Rongsheng Xu Chief Scientist, National Computer Network Intrusion Protection Center, China

CFET 2008 Conference Schedule

Day 1 –1st September 2008

10.00 - 10.30 **Registration & Coffee – foyer Powell Building**

10.30 - 10.45 **Welcome to the Conference – Powell Lecture Theatre**

Professor Michael Wright, Vice Chancellor
Canterbury Christ Church University, UK

Denis Edgar-Nevill, Chair CFET 2008
Canterbury Christ Church University, UK

10.45 - 11.30 **Invited Keynote Presentation – Powell Lecture Theatre**


Professor Nigel Jones MBE
Adjunct Professor University College Dublin, Republic of Ireland
Director, Technology Risk Limited, UK

11.30 – 13.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

"Cybercrime – Awareness is Protection"
Margaret Ross
Southampton Solent University, UK

"Extending the Multidisciplinary Learning Experience in Digital Forensics Using Mock Trials"
Gary C. Kessler
Champlain College, USA

"An Investigation into the Social, Legal and Ethical Issues Associated with Biometrics in the UK"
Lynne Norris-Jones
University of Wales Institute, UK

Powell Pg06 Lecture Theatre

"An Investigation into the Vulnerabilities of Computer Forensic Processes as shown through an Anti Forensics Tool"
Paula Thomas & Christy Petersen
University of Glamorgan, UK

"New methodology in facial composite construction and the associated implications for facial ID training"
Dr. Stuart Gibson Dr. Christopher Solomon and Mr. Clifford Clark
University of Kent and New Zealand Police, UK & New Zealand

"An analysis of the accuracy and usefulness of Vinetto, Pasco and Mork.pl" Dave Childs & Paul Stephens
Digital Evidence Recovery & Internet Crime Lab, Trading Standards & Regulatory Services and Canterbury Christ Church University, UK

13.00 - 14.00 **Lunch**

14.00 – 14.45 **Invited Keynote Presentation – Powell Lecture Theatre**


Stephen Mason
Visiting Research Fellow at the
British Institute of International and Comparative Law

14.45 - 15.30 **Coffee & Exhibitors - Powel Foyer and Pg05**

15.30 – 17.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

"A Swedish IT Forensics Course - Expert Opinions"
Rein Oja & Alan Davidson
Stockholm University and the Royal Institute of Technology, Sweden

"Development of a Masters module in Computer Forensics and Cybercrime" Richard E Overill
King's College London, UK

"Virtual Reality Police Training: How much visual information is too much?"
Iwan Kartiko and Manolya Kavakli
Macquarie University, Australia

Powell Pg06 Lecture Theatre

"Cyber Fraud in Ghana locally known in the Hausa language as "SAKAWA" An ethnographic Study of a Popular Slum community in Ghana- Nima"
Koranteng, Kweku Oduro
University of Ghana, Ghana

"Developing a Digital Forensic Framework for a Third World Country"
Kasun De Zoysa, Keerthi Goonathillake, Ravith Botejue
University of Colombo, Sri Lanka

"What can a computer forensics examiner learn from an ethical hacker?"
Paul Stephens & Gerald Stock
Canterbury Christ Church University, UK

Powell Pf07 Lecture Theatre

"Building the Infrastructure to Support HE Computer Forensics"
Denis Edgar-Nevill
Canterbury Christ Church University, UK

"The importance of funding and training to manage and investigate computer crime"
Hamid Jahankhani, Amie Taal, Ian Mitchell
Middlesex University, UK

"Cybercrime Legislation in China"
Man Qi, Yongquan Wang, Rongsheng Xu
Canterbury Christ Church University, East China University of Political Science and Law, Chinese Academy of Sciences, China

18.30 – 19.00 **Drinks Reception**

Blue Room and the Senior Common Room of the North Holmes Rd Campus of Canterbury Christ Church University.

19.00- 21.00 **Conference Dinner**

Blue Room and the Senior Common Room of the North Holmes Rd Campus of Canterbury Christ Church University.

Menu

Starters
Prawn & avocado salad with lardoons of bacon

Main courses
Grilled salmon with a Béarnaise Sauce
with seasonal vegetables & potatoes

Vegetarian - Ratatouille stuffed Beef Tomatoes served with Tomato Sauce

Desserts
Passion Fruit Bavarois

~~~

Cheese & Biscuits

Coffee and Teas
~~~

Day 2 – 2nd September 2008

09.00 – 09.45 **Invited Keynote Presentation – Powell Lecture Theatre**

"Computing 'Environment': It's more than Binary Code – It's About Criminals!!

Edward P. Gibson
Chief Security Advisor Microsoft Ltd, UK

09.45 – 10.45 **Parallel Presentation Sessions**

Powell Lecture Theatre

"Mobile Phone Forensic Investigation – Technical and Legal Challenges"
Abhaya Induruwa
Canterbury Christ Church University, UK

"XFT – A Forensic Toolkit for the Original Xbox Game Console"
David Collins
Sam Houston State University, USA

Powell Pg06 Lecture Theatre

"Digital Evidence Analysis in China"
Zhijun Liu, Ning Wang, Yonghao Mai, Huanguo Zhang
Hubei University of Police; Wuhan University Computer School;
Key Laboratory of Computer Forensics, China

"Is Property Theft in Crime Investigation? Using OSS in Cybercrime Education"
David Bennett and Paul Stephens
Canterbury Christ Church University, UK

Powell Pf07 Lecture Theatre

"Understanding digital certificates"
George Weir
University of Strathclyde, UK

"The Social Effects of Spam"
Reza Mousoli, Dr Man Qi, Denis Edgar-Nevill
Canterbury Christ Church University, UK

10.45 – 11.15 **Coffee & Exhibitors - Powel Foyer and Powell Pg05**

11.15 – 12.45 **Parallel Presentation Sessions**

Powell Lecture Theatre

"Virtual environments have a prominent role in securing your organization: Case Study on a DDoS attack"
Righard Zwienenberg
Norman Data Defence Systems Ltd, UK

"Egregious use of Tor Servers? Data retention, anonymity, and privacy on-line"
F.W.J. van Geelkerken
Tilburg University, The Netherlands

"Comparison of Drupal and Joomla security functions for designing secure Content Management System"
Reza Mousoli
Canterbury Christ Church University, UK

Powell Pg06 Lecture Theatre

"Case-oriented evidence mining in forensic computing: A case study"
Jun Zhang & Lina Wang
Wuhan University, China College of Police, Hubei, China

"A Case-Based Reasoning Model for Digital Intrusion Forensics"
Zeming Yang, Rongsheng Xu, Man Qi
Chinese Academy of Sciences, Canterbury Christ Church University China & UK

12.45 - 14.00 **Lunch**

14.00 - 14.45 **Invited Keynote Presentation – Powell Lecture Theatre**

"Digital Forensics Research in China"

Professor Rongsheng Xu
Network Security Group
Institute of High Energy Physics
Chinese Academy of Sciences, China

14.45 - 15.30 **Plenary Panel Session - Powell Lecture Theatre**

15.30—16.00 **Coffee & Exhibitors**

1600 **Conference Close**

Presentation Abstracts – 1st September 2008

Invited Keynote Presentation

Professor Nigel Jones MBE
Adjunct Professor University College Dublin, Republic of Ireland
Director, Technology Risk Limited, UK

Cybercrime – Awareness is Protection

Margaret Ross, Geoff Staples, Mark Udall
Southampton Solent University, Faculty of Technology,
East Park Terrace, Southampton, S014 6RD
E-mail: Margaret.Ross@Solent.ac.uk

Abstract

One of the many approaches to enable businesses and individuals to protect themselves from the ever-increasing amount and range of cybercrime, is by education. This is relevant to students studying different aspects of undergraduate and postgraduate computing. The approaches used to raise this awareness, from first year IT undergraduates to Master students, none of whom are cybercrime or security specialists, are considered. These students specialise in different aspects of computing from business information systems, through software development to networking.

Extending the Multidisciplinary Learning Experience in Digital Forensics Using Mock Trials

Gary C. Kessler
Champlain College
Burlington, Vermont, USA
gary.kessler@champlain.edu

Abstract

Computer forensics in a multidisciplinary, hands-on field of study and nothing reinforces this more for the student than opportunities to practice the skills while working with counterparts in other fields. The computer forensics process includes identification, preservation, acquisition, examination, analysis, and reporting, with the last being the most visible to others; if reporting and testimony are poor, even the best examination can be compromised and the results called into question.

Although our computer forensics curriculum requires students to take courses in computer technology, networking, and criminal justice in addition to fundamental computer forensics and digital investigation courses, we have started to employ a large mock trial event to bring students from different disciplines together for a major final project. The scenario is pre-planned by advisers from the computer forensics, criminal justice, and paralegal faculty. The actual incident starts with a crime scene, staged by volunteers from the college's performing arts students and set by the Crime Scene Investigation instructor; only the suspect and victim know what is supposed to happen and the witnesses are not primed as to what to expect. Criminal Justice students secure and process the crime scene, interview witnesses, and gather evidence. In the process, mobile phones and USB thumb drives are found and the criminal investigators work with the Computer Forensics students to write an appropriate search warrant for those devices. Computer Forensics students forensically process the digital devices, providing a report of their analysis to the criminal investigators. All reports are forwarded to Paralegal students who work with local attorneys who act in the role of the prosecution and defense teams. On the day of the trial, a retired criminal court judge presides over the proceedings, complete with a jury selected from volunteers from the college community. For many students, this is the first trial scenario they have seen outside of television, and the attorneys and judge ensure realism.

The best learning experience for the students is to see how difficult the actual process is. In particular, the difficulty in testifying, professionally conveying the proper message, and dealing with a possibly hostile cross-examination is surprisingly difficult. Students also learn that the evidence does not always speak for itself to gain convictions; in two trials, both defendants -- who did, in fact, commit the crime for which they were accused -- have been found not guilty.

This paper will describe the mock trial process that we have employed including the components of setting the stage, gathering partners, scheduling, and establishing the actual crime scene. Particular emphasis will be placed on the digital evidence that was prepared to match the scenario but, purposely, have elements that are open to interpretation. Lessons learned from the past and plans for future trials and integrating them more tightly into the classroom will also be discussed.

An Investigation into the Social, Legal and Ethical Issues Associated with Biometrics in the UK (Practical Application to Computing Programmes)

Lynne Norris-Jones
University of Wales Institute, UK

Abstract

This paper begins with a review of the Biometric applications currently in existence and discusses some of their major social, legal and ethical implications traced largely from the landmark date associated with world security following the September 11th attack on the World Trade Centre. This incident led to more stringent calls for biometric technology to develop consistently to ensure the security of systems worldwide. Biometrics is recognised as an ever expanding area, currently associated with a whole spectrum of practical applications. The technology ranges from physiological biometrics, including fingerprinting, iris and retina scanning, to behavioural biometrics for keystroke, signature and vocal pattern. This technology may provide secure authentication and identification for improved security but it poses a range of legal, social and ethical issues. Primary concerns stem from the fear of relinquishing human rights to privacy and general intrusion into personal life both currently and in the future with further development of biometric technology. This research area aims to investigate appropriate teaching and learning strategies to meet the needs of industry, via the training of potential practitioners in this area. It aims to raise awareness of the major implications of biometric implementation within society and foster strategies to respond to practical implications, with an appropriate strategy being incorporated into a Biometrics module for level III undergraduate students. The primary investigation uses an interpretive paradigm whereby a series of scenarios are developed based on issues posing a range of social, legal and ethical implications for society, using a series of focus group meetings and interviews with students of the developing Biometrics module and associated teaching staff. This inductive approach (Ticehurst & Veal, 1999) relies upon the participants of the study providing their own explanation and interpretation of the situation being studied, representing a reliable basis for practitioner reflection of the issues under investigation and associated reflection upon some appropriate responses to the issues. The aims of this paper are three-fold: to investigate the emergence and practical implications of biometric technology; to justify the need to develop and implement a biometrics programme for delivery to level III undergraduates and to develop an appropriate set of teaching and learning strategies to meet the professional needs of potential practitioners of Biometric technology. In order to achieve the aims, a multi-modal approach of case studies and focus group meetings was used. A number of specific issues were addressed in the case studies whereby two separate scenarios were presented to two groups (one full-time group and one part-time group for each set of scenarios) with two students in each group, in order that they may arrive at some specific phenomena (Silverman, 2007) and this was triangulated with a series of two general Focus Group discussions, to gain a more complex understanding of participants' perceptions of emerging Biometric technology and its practical implications (Creswell, 2007). The findings from the study were used to refine the indicative content and learning outcomes of the Biometrics module and to prepare for the delivery of the module in the academic session 2008-09.

An Investigation into the Vulnerabilities of Computer Forensic Processes as shown through an Anti Forensics Tool

Paula Thomas & Christy Petersen,
Faculty of Advanced Technology,
University of Glamorgan, Pontypridd, UK, CF37 1DL,
pthomas@glam.ac.uk, chrpet@hotmail.com

Abstract

Computer forensics has gone from being a fairly new technology, to something that is now frequently relied upon as a method of establishing factual information as evidence in a court of law. Due to its new found importance in today's criminal environment, people can often put absolute trust into computer forensic tools and processes, believing that the evidence obtained is absolutely true. It is argued that there is too much dependence on computer forensic tools and that computer forensic analyst's don't actually know just how effective these tools are. This is where anti forensics can be so important, because the best way of evaluating something, is by challenging it. Anti forensics can be defined as the intentional alteration and modification of data in attempt to reduce the quality and quantity of evidence. This makes it more difficult for computer forensic investigators to positively identify valid pieces of evidence.

The aim of this work is to assess the extent to which computer forensic investigations could be affected through the use of anti forensics and then to develop a prototype anti forensics tool to display these weaknesses. The tool will be able to create a user defined amount of files on a Windows XP system and encrypt them, thus providing false and misleading evidence. This tool will be able to successfully prolong forensic investigations by populating a computer system with a significant number of bogus files. The file content can be either default (filling a file with useless data) or it could be personalised content, and used as a quick method of hiding and encrypting evidence. The actual file creation will be randomly generated and the tool will then automatically encrypt them. Encrypting certain files will mislead the forensic investigators into thinking that they have some sort of relevance to the case. Decrypting the irrelevant files could be a timely process.

It is anticipated that the tool to be created will be able to successfully exploit the computer forensic process and to clearly demonstrate its ability to over complicate the work flow process of even the most experienced computer forensic analyst.

New methodology in facial composite construction and the associated implications for facial ID training

Dr. Stuart Gibson (University of Kent), Dr. Christopher Solomon (University of Kent) and Mr. Clifford Clark (New Zealand Police)

Abstract

A facial composite is a graphical representation of a suspect's face that is generated from an eyewitness's memory. In the absence of other forensic evidence, a facial composite may constitute the only means of locating a suspect. Computerised techniques for constructing facial composites such as E-FIT (Electronic Facial Identification Technique) are essentially electronic versions of the original mechanical feature-based systems, introduced in the 1970's (PhotoFIT and Identikit). Although these computerised systems have proved successful since their inception in 1980's the effectiveness of the feature-based approach is fundamentally limited by the witness's ability to recall and verbalise accurate descriptions of facial features from memory. For this reason an emphasis has been placed on the need to train composite operators in cognitive interview techniques (Fisher & Geiselman). In fact, the cognitive interview typically currently constitutes more than 50% of a composite operator's training. New advances in facial composite methodology have led to software systems that do not rely on the witness's ability to provide detailed facial descriptions but instead utilises the, cognitively less demanding, process of recognition. The new methodology has implications for training programmes and the Association of Chief Police Officers (ACPO) Guidelines on Facial Identification.

In this paper we compare the technical and operational differences between the traditional feature-based approach to facial composite construction and the new methodology. Justification for the new approach is based on previous cognitive psychology research and feedback from two UK police constabularies who have adopted a new facial composite system called EFIT-V. The training requirements for the new system are presented in the context of existing facial ID training and its use in higher education as a research tool and learning package are also discussed.

An analysis of the accuracy and usefulness of Vinetto, Pasco and Mork.pl

Dave Childs
Lab Manager, Digital Evidence Recovery & Internet Crime Lab, Trading Standards & Regulatory Services, Email: dave.childs@northyorks.gov.uk
&
Paul Stephens
Programme Director BSc (Hons) Forensic Computing, Department of Computing, Canterbury Christ Church University, Email: paul.stephens@canterbury.ac.uk

Abstract

The majority of forensic examiners in the UK use a Microsoft Windows-based platform together with a proprietary forensic application to carry out their analyses. These commercial forensic software packages tend to carry considerable licensing costs, as does the Windows operating system itself. In comparison, Linux is free and contains many forensically useful native tools. Additionally, there are free and open source applications available that have been created specifically for use in computer forensics examinations. This paper assesses the accuracy and usefulness of three such tools: Vinetto[1], Pasco [2] and Mork.pl[3].

In order to do this, tests were carried out using the three packages, each written to analyse a particular software artefact: Vinetto – a Thumbs.db thumbnail file; Pasco – an Index.dat Internet Explorer history file; and Mork.pl – a History.dat Mozilla Internet history file. The same files analysed by the free tools were then examined using commercial, Windows-based forensic software and the results compared.

Whilst the amount of information recovered from the free and commercial tools was roughly the same, the commercial tools tended to offer more flexibility in terms of presentation and reporting. Netanalysis [4], for instance, includes the ability to automatically recreate cached web pages from the Internet Explorer Index.dat file and cache folders, which gives it a significant advantage over its free tool equivalent.

Within the forensic discipline, accuracy of information is vital and the examination of the Thumbs.db thumbnail file showed there to be an inaccuracy with the time/date reporting of Guidance Software's Encase [5]. If a forensic analyst were to rely on the information presented by Encase, without being aware of its inaccuracy, their results would be incorrect. In this case, the free tool provided the same amount of data as its commercial rival, but, crucially, it provided accurate data where Encase had not.

Whilst the analyst who is familiar with their commercial, Windows tools, is unlikely to switch completely to a Linux-based platform, they may well consider investing the time necessary to learn how to use these free tools in order to have an alternate platform to test and validate their results.

Selected Bibliography

[1] Roukine, M. (2007) *Vinetto : a forensics tool to examine Thumbs.db files*. Available at: http://vinetto.sourceforge.net/ (Accessed: 5th October 2007).

[2] Jones, K. J. (2007) *Foundstone, Inc.© Pasco*. Available at: http://www.foundstone.com/us/resources/proddesc/pasco.htm (Accessed: 5th October 2007).

[3] Zawinski, J. (2007) *marginal hacks*. Available at: http://www.jwz.org/hacks/marginal.html (Accessed: 5th October 2007).

[4] Digital Detective. (2007) *Digital Detective - Forensic Computing Tools and Utilities*. Available at: http://www.digital-detective.co.uk/netanalysis.asp (Accessed: 13th October 2007).

[5] Guidance Software. (2007a) *EnCase® Forensic*. Available at: http://www.guidancesoftware.com/products/ef_index.aspx (Accessed: 8th September 2007).

Invited Keynote Presentation

Stephen Mason

Visiting Research Fellow at the
British Institute of International and Comparative Law

Stephen is barrister (www.stephenmason.eu) and a member of the IT Panel of the General Council of the Bar of England and Wales and the UK representative on the IT Law Committee of the Council of Bars and Law Societies of Europe. He is the general editor of *Electronic Evidence: Disclosure, Discovery & Admissibility* (LexisNexis Butterworths, 2007) and *International Electronic Evidence*, (British Institute of International and Comparative Law, 2008). He is the author of *Electronic Signatures in Law* (Tottel, 2nd edn, 2007) and *E-Mail, Networks and the Internet: A Concise Guide to Compliance with the Law* (xpl publishing, 6th edn, 2006). He is the founder and general editor of the *Digital Evidence and Electronic Signature Law Review*.

A Swedish IT Forensics Course - Expert Opinions

Rein Oja & Alan Davidson
The Department of Computer and Systems Sciences,
Stockholm University and the Royal Institute of Technology

Abstract

There is mounting pressure for institutes of higher education to fill society's need for qualified IT forensics practitioners. Some of the more suitable candidates for providing such education are those departments that already have a history of teaching the subject of IT security. Many of the technical issues that are of relevance to IT forensics are already covered in the normal IT security curriculum. However, IT forensics is clearly a broad subject that should span far more than relevant technical procedures and tools. A survey of the available literature on the subject of IT forensics reveals that the majority is written for English speaking countries, and is consequently related to the legal systems and procedures in those countries. One can suspect that the core of the subject is dependent on the legal system it is applied within, and it is therefore not immediately apparent how applicable the available literature is for the curriculum of a course held in Sweden.

Beginning with the assumption that Security Laboratory at the Department of Computer and Systems Sciences, Stockholm University should include a five week course in IT forensics within its course catalogue, we investigated what a suitable course content would be - from a Swedish perspective. We also sought answers to what literature and tools would be suitable to support such course content. Besides a survey of the relevant available literature, a series of five interviews with Swedish legal experts and computer forensic professionals were conducted from late 2006 and into 2007. Among the interviewees were both the Swedish law enforcement departments; the attorneys office and the police, and private Swedish IT-companies. Despite differences in the legal systems, the results from the literature study and the interviews did not differ significantly. One point where the results do nevertheless differ is whether criminology should be included; it is often a part of the literature but the interviewees did not regard it as important. Somewhat unexpected was the fact that the answers between the interviewees differed depending on whether they represented the public legal system or the IT industry. One question that clearly divided these groups was whether teaching ethical issues of the subject should be included or not.

Development of a Masters module in Computer Forensics and Cybercrime

Richard E Overill
Department of Computer Science, King's College London,
The Strand, London,
WC2R 2LS, UK

Abstract

In mid-2004 it was decided that the list of optional modules available to students taking the MSc programme in Computing, Internet Law and Management at King's College London should be supplemented with a module in Computer Forensics and Cybercrime. It was proposed that this module should be delivered as a reading course to be assessed by means of a dissertation and a linked *viva voce* examination.

We trace the evolution of this module over the three academic years 2005/6 to 2007/8 inclusive and discuss the range of dissertation topics selected by the students. The results obtained by the students and the evidence from anonymous student feedback surveys are analysed quantitatively. We conclude with a critical assessment of the success of the module in meeting its specified aims and objectives and put forward proposals for its future development.

Virtual Reality Police Training: How much visual information is too much?

Iwan Kartiko and Manolya Kavakli
VISOR (Virtual and Interactive Simulations of Reality) Research Group,
Department of Computing
Macquarie University
Sydney NSW 2109 Australia

Abstract

The advancement of computing technology has enabled researchers to develop complex Virtual Reality (VR) systems with relatively less effort to traditional methods for police training. Institutions utilise the advantages of VR to train police and military officers. In this article, we propose to consider Cognitive Theory of Multimedia Learning (CTML) in the development of VR simulations for police training. CTML suggests ways to manage cognitive load originated from excessive use of visual information. This has severe implications on the learning outcome. While complex visual information could be overwhelming, too simple visual information could totally eliminate the benefits expected in this learning process. In this paper, our aim is to investigate how much visual information is too much. Most VR applications crave for the generation of the most realistic real-world representations as much as possible. Is this necessary?

Many theories has been proposed from cognitive load point of view, which give an idea of how humans process information. This leads to several multimedia learning theories and instructional design principles from many researchers (e.g.Mayer, 2001; Mayer and Moreno, 2002a; Moreno, 2006; Moreno and Mayer, 2007). While the notion of "Learning" itself is commonly perceived as an activity to acquire knowledge, "Training" is perceived as a process of learning to attain a specific job-related skill. Mayer (2001) suggests three types of learning outcomes: no learning, rote learning and meaningful learning. These outcomes are based on measures of three variables: recall, retention and transfer. Recall is a straight-forward memorisation of material. Retention is the comprehension level of the material. Transfer is the ability to use knowledge gained to answer related problems that is not directly answerable from material content. According to Mayer, no learning occurs where retention and transfer are low, but recall may be high, indicating strict memorization but no learning. Rote learning is when recall and retention are high, but transfer measures are low. In rote learning, material has been received but not well integrated with prior knowledge. This still suggests that only memorisation occurred. The significant outcome of learning is meaningful learning. In meaningful learning retention and transfer are high, but, recall scores are often low due to the significant processing of original information and the integration of this information with prior knowledge. Mayer suggested that the more integration that occurs the less likely a learner will be able to recall original information provided. High transfer score also indicates a high level of understanding of the material to be learned. Understanding and learning may be correlated, however they are fundamentally different as the former can happen without the latter (Schnotz and Kürschner, 2007).

To measure learning outcome we have developed a virtual reality training system, BOSS (BOrder Security Simulation) for training police officers at a virtual airport, using an

immersive semi-cylindrical projection system (VISOR: Virtual and Interactive Simulation of Reality) and a set of animations using Vizard Virtual Reality Software in our Virtual Reality Systems (VRS) Lab. Police officers are expected to interact with virtual actors as visual information providers in a virtual airport model. The use of entities to enrich a virtual environment for a real-time purpose must be planned carefully. Resource limitations, such as; computer memory, graphic processors and main processor capabilities must be addressed carefully (Kavakli and Kartiko, 2007). Otherwise, the simulation in the virtual environment will not run at full speed and will lag, and affect the user experience and performance (Glencross et al., 2006; Harrington, 2006). So, addressing the use of entities or the quality of virtual objects is of great importance in a virtual reality application. In this paper, we describe the requirements of a police training simulation, in the light of CTML to provide meaningful learning outcomes in the domain of Policing, drawing results from a set of experiments that involve various types of animations with different levels of visual information.

Cyber Fraud in Ghana locally known in the Hausa language as “SAKAWA” An ethnographic Study of a Popular Slum community in Ghana-Nima

Koranteng, Kweku Oduro
Information Communication Technology Directorate,
University of Ghana, Legon. P.O. Box LG25, Legon
kkoranteng@ug.edu.gh, kweku.koranteng@gmail.com

Abstract

Cyber crime as an area of study has received little or no attention in developing countries round the world where significant proportions of these Internet crimes take place. One of the major issues battling the advancement of Information and Communication Technology in developing countries in general has been the non-existing regulatory framework to control and monitor the advancement ICT in respective countries. In Ghana, like many other developing countries, enforcement and regulation of laws in this area has been a daunting task. Even though Ghana is among the very few African countries with a draft policy on ICT, the issue with regulation has been viewed with lots of skepticism in many quarters. Notwithstanding these setbacks, Governments of Ghana is still poised to ensure equity in the implementation of its ICT programs and policies to facilitate the development of its economy. Government over the years have come to the realization that before their economies can reap total benefit of global economic business exchange in this 21st century, they will have to bring their segmented economies onto a global platform through ICT. Nonetheless, the indispensable nature of ICT in Ghana's economic development has triggered series of policy formulation in other sectors of the economy. National ICT policies formulated in 2005 did set in motion a good basis for the development of ICT in all sectors; education, health care delivery, governance etc. Despite the great strides made by national governments to ensure equitable access to ICT infrastructure, much attention is not paid to the threat these technologies pose to national security and state sovereignty. African Cyber crime Enterprises, for that matter West African Cyber crime syndicates are among one of the most active and vibrant crime syndicates in the world. Significant among these are the Nigerian Cyber crime Enterprises. Ghana, the first black sub-Saharan to gain independence from Britain in 1957, one of the emerging economies in Africa today, and referred to in many economic quarters as the gateway to West Africa, is rather and gradually becoming a safe haven for the perpetuation of all forms of crimes; illegal migration, drug-traffic and cyber related crimes. The research takes an ethnographic view of cyber fraud carried out in Ghana, specifically within a slum community in Ghana-Nima, which is noted as one of the most notorious hideout for most West African migrant. ‘Nima’ as the slum is called, geographically, lays in the heart of the Accra the capital of Ghana and about 15 minutes drive from the Kotoka International Airport. The total population size of this community is estimated to be about 50,000 inhabitants. Nima extends into neighbouring communities such as Kokomlemle, Malata, Kanda, New Town, Pigfarm, Kotobabi and Mamobi

Developing a Digital Forensic Framework for a Third World Country

Kasun De Zoysa[1], Keerthi Goonathillake[2], Ravith Botejue[3]
[1]University of Colombo School of Computing
No 35, Reid Avenue, Colombo 07, Sri Lanka.
kasun@ucsc.cmb.ac.lk
[2]University of Colombo School of Computing
No 35, Reid Avenue Colombo 07. Sri Lanka.
keerthi@ucsc.cmb.ac.lk
[3]Lanka Software Foundation
1st Floor, UCSC Building, No. 35, Reid Avenue
Colombo 07. Sri Lanka.
ravithb@yahoo.com

Abstract

Due to the increased number of computer related and cyber crimes reported in third world countries, within the past few years, digital forensics has become a key area in law enforcement. A digital forensic framework compatible with a country's legislation is a must when digital forensics are used in investigating crimes.

This paper is a review of several digital forensic frameworks / models that are currently existing in order to develop an abstract digital forensic process model that would be suitable to be used with the current legislation of a developing country such as Sri Lanka. It identifies core areas of different forensic models and explains why some activities addressed in them become impractical in the context of Sri Lanka. The paper uses several computer related and cyber crime cases reported from the year 2003 to justify the authors' views.

What can a computer forensics examiner learn from an ethical hacker?

Paul Stephens & Gerald Stock
Department of Computing, Canterbury Christ Church University

Abstract

In recent years, two new yet related subject areas have emerged namely ethical hacking and computer forensics. Ethical hacking degree programmes have appeared at universities such as the University of Abertay Dundee [1], Northumbria University [2], and Coventry University [3]; whilst computer forensics has over twenty undergraduate programmes across the UK [4]. In addition, there are several training courses associated with both ethical hacking and computer forensics. For ethical hacking, perhaps the best known is the Certified Ethical Hacker (CEH) programme offered by the EC-Council [5]. While for computer forensics a number of training courses are available including those for proprietary software, such as the EnCase Certified Examiner (EnCE) [6], and more general courses such as those run jointly by Canterbury Christ Church University (CCCU) and the National Policing Improvement Agency (NPIA) validated as an MSc in Cybercrime Forensics [7]. This paper explores the similarities and differences between the EC-Council's CEH programme and the MSc in Cybercrime Forensics run jointly by CCCU and the NPIA, concluding that a computer forensics examiner can learn much from an ethical hacker. This is because ethical hacking places an emphasis on intelligence gathering, as does the current political climate associated with the so called 'War on Terror' following '9/11'. Although this may be good from a policing and intelligence standpoint one of the casualties of this war could be our civil liberties.

Selected Bibliography

[1] University of Abertay Dundee. *BSc (Hons) Ethical Hacking & Countermeasures*. Available at: http://www.abertay.ac.uk/Courses/CDetails.cfm?CID=363&Key=003.002 (Accessed: 28th April 2008).

[2] Northumbria University. *Ethical Hacking BSc (Hons) - Course Information - Northumbria University, UK*. Available at: http://northumbria.ac.uk/?view=CourseDetail&code=UUSETH1.

[3] Coventry University. *Ethical Hacking and Network Security degree*. Available at: http://www.coventry.ac.uk/undergraduate-study/full-time-courses-by-subject/internet,-mobile-and-network-computing/a/2793#top (Accessed: 28th April 2008).

[4] UCAS (2008) *UCAS course search*. Available at: http://search.ucas.co.uk/cgi-bin/hsrun/search/search/StateId/DZF7_39X-az4R5O2bl9GrBNkCk59E-4-7R/HAHTpage/search.HsKeywordSuggestion.whereNext?query=5179&word=FORENSIC+COMPUTING&single=N (Accessed: 28th April 2008).

[5] EC-Council (2008) *EC-Council | Certified Ethical Hacker*. Available at: http://www.eccouncil.org/ceh.htm (Accessed: 28th April 2008).

[6] Guidance Software (2008) *Guidance Software Professional Development and Training*. Available at: http://www.guidancesoftware.com/training/EnCE_certification.aspx (Accessed: 28th April 2008).

[7] CCCU (2008) *Canterbury Christ Church University - Courses and Prospectus - Postgraduate Courses*. Available at: http://www.canterbury.ac.uk/courses/prospectus/postgraduate/courses/cybercrime.asp (Accessed: 28th April 2008).

Building the Infrastructure to Support HE Computer Forensics

Denis Edgar-Nevill
Canterbury Christ Church University, UK

Abstract

Creating new university courses to support new disciplines is difficult. It relies upon a degree of commitment and belief from those involved. By far the larger part of this is the commitment from university management in creating an infrastructure to support the delivery; particularly in case of technology based courses such as with computer forensics. It is a gamble.

This paper discusses the history of development of computer forensics in the Department of Computing at Canterbury Christ Church University. A new MSc in Cybercrime Forensics was established in 2003 followed by an undergraduate provision in 2007. It has been a constant problem in balancing the competing demands of the student marketplace, competing university courses and the swings and roundabouts in changes of government funding policies and the attitudes of employers to the developmental needs of their staff. Throughout this process the goal has been to establish a critical-mass of expertise and resources in creating a sustainable infrastructure.

The importance of funding and training to manage and investigate computer crime

Hamid Jahankhani, *Amie Taal, Ian Mitchell
Middlesex University, UK
{h.jahankhani, I.Mitchell}@mdx.ac.uk
*Ex law enforcement officer, Serious Fraud office, UK

Abstract

Fuelled by frequent sensational media headlines and news coverage of cyber-crime in the UK and the lack of enough police action, this paper attempts to provide an unbiased perspective from the law enforcement arena, critically assessing the importance of funding, proper education and training to handle, manage and investigate computer evidence and lastly the importance of having a form of accreditation to validate experience, skills and qualifications and this was achieved.

Keywords: Computer Forensics, Digital Forensics, Computer Forensic Consultant, Expert Witness, Computer Law Enforcement Agents, Government, E-Crime, Cyber-Crime, Training, Funding

Cybercrime Legislations in China

Man Qi[1], Yongquan Wang[2], Rongsheng Xu[3]
[1]Department of Computing, Canterbury Christ Church University, Canterbury, UK
man.qi@canterbury.ac.uk
[2]School of Information Science and Technology, East China University of Political Science and Law, Shanghai, China
wangyongquan@ecupl.edu.cn
[3]Institute of High Energy Physics, Chinese Academy of Sciences, Beijing, China
xurs@ihep.ac.cn

Abstract

Computer and network development has been so rapid and dynamic these years in China. According to authorized international report, China has the most Internet users in the world. The internet has become indispensable for the daily personal activities of millions of ordinary people.

However this trend has also expedited an exponential development of new crime in cyberspace. And the existing legal framework in China is insufficient to serve the changes. The Internet related regulations put forth so far tend to be on a reactive mode.

The paper provides an overview of cybercrime legislations in China, starting from the history of computer and network development, cybercrime development and corresponding legislation development in China. Then the detail of the legislation system is given based on a supposed classification.

Cybercrime has been paid concerns in China with the spread of network. Just as computer and network technology came later in China than in western countries, the relevant cybercrime legislations came as late as mid 90s'. The legal system includes substantive criminal law, supplemented by the relevant regulations and commercial and intellectual property protection laws. They may work together to prohibit misconducts directed towards or involving computers or associated information technology. However, the gaps and inadequacies in the provisions necessitate the consideration of more specific laws targeting cybercrime.

The legislation system development should also consider the differing legal, social and political contexts and emphasize aspects of effective policing and enforcement that go beyond criminal or penal sanctions.

Presentation Abstracts – 2nd September 2008

Invited Keynote Presentation

"Computing 'Environment': It's more than Binary Code – It's About Criminals!!"

Edward P. Gibson
Chief Security Advisor Microsoft Ltd, UK

Despite the mutating threats of cyber attacks, online extortion, or spam, a well-structured information security strategy can safeguard your business and ensure that risks are managed with commitment and understanding. It can also help to reassure your customers, who in the UK (for example) according to a recent study now fear internet crime more than burglary, mugging or car theft. Yet, because the internet is not territorial or jurisdictionally bound, organized crime efforts to steal everything you hold dear by extortion, threats, intimidation – not in the bricks and mortar world but in the online world, our normal responses to 'attack' are not as effective. But there are solutions . . . and sometimes they are free. Ed Gibson will give you a peek inside his 'cyber life' utilizing anecdotes from his 20 year career with the FBI including the most recent 5 years when he was assigned as a Diplomat to the US Embassy London in charge of all the FBI's cyber investigations in the UK.

Biography

Mr Gibson's primary role is to serve as the senior advisor to Microsoft's customers, partners, government elites, and the public on how to best respond to the current security environment - from internal leakage of intellectual property to best practices for online cyber security - and how to improve their security through Microsoft's solutions and services. As Microsoft's Trustworthy Computing (TWC) initiative continues, one of the key skills Mr Gibson brings to Microsoft is his ability to forge and maintain strategic alliances across public and private sector organisations in an international environment. He is the link between Microsoft and industry specialists, law enforcement, government and academia, facilitating the sharing of security knowledge between these groups. Ed's experience and knowledge was gained through a 20-year career as a Special Agent with the Federal Bureau of Investigation (FBI). During this period, he was a recognized expert in investigating international money laundering & fraud schemes, economic espionage, and intellectual property theft. From early 2000 - June 2005, Mr Gibson was assigned to the American Embassy in London where he served as the FBI's Assistant Legal Attaché in the UK and Ireland. During this period Gibson was responsible for all FBI hi-tech, Internet extortion, blackmail, cyber terrorism, intellectual property theft, crimes against children, and infrastructure protection investigations. His focus on how criminals exploit the internet and his investigative abilities have made him an ideal figurehead for Microsoft's efforts in secure computing. Before his appointment to the FBI, Mr Gibson served for five years as an in-house lawyer for a multi-national corporation based in the USA. He is a qualified Solicitor in England and Wales, has completed a 2-year computing program at Oxford University, serves on several technology association steering committees and advisory boards, and is a Fellow of the British Computer Society.Since taking on his role with Microsoft UK, Ed has lectured widely on cyber-threats, internet crime, social networks, and e-business. He is a sought after speaker given his ability to bring security to life and make it personal. You can contact Ed by e-mail at EdGibson@Microsoft.com

Mobile Phone Forensic Investigation Technical and Legal Challenges

Abhaya Induruwa
Department of Computing
Canterbury Christ Church University
Canterbury
United Kingdom

Abstract

The proliferation of mobile phones in the world is incredible. Over the last twenty years the number of users has grown from a mere handful to billions, the last billion being added in less than two years. This corresponds to 1000 new customers signing up for mobile services every minute around the world. By the end of 2007 there have been more than three billion mobile phone subscriptions worldwide. This includes 70 million in the UK and 666 million in Europe. 65% of handsets made are expected to be sold in the emerging markets in Africa, Asia and China. Consequently the use of mobile phones connected to criminal activity is on the increase.

There is no single market that has felt the increase in pace of technology as much as the mobile phone industry. Manufacturers continue to push technological boundaries and pack more features into mobile phones. The specifications of mobile devices in terms of memory, storage and connection speed are being enhanced at an unprecedented rate. The absence of a standard operating system adds to the complexity of examination process and understanding of the data recovered. This has made it difficult for the developers of forensic investigation tools to keep pace with changing mobile technologies and capabilities of modern day devices. The forensic examination of a mobile phone is complicated by the fact that each model requires different analysis tools and investigative techniques. Moreover the ease of use of a mobile in any part of the world using international roaming brings another dimension to the investigations of mobile devices connected to crimes. As a result the Forensic investigators examining and analysing mobile devices face a multitude of difficulties.

Mobile phone forensics investigation is a relatively new field yet it is an important aid to law enforcement. This paper outlines the challenges faced by the Mobile Phone Forensics Examiner/Investigator and illustrates the relevance of ACPO guidelines applicable in the UK to the Examiners/Investigators in carrying out proper examinations/investigations. It then discusses different models and practices developed or adopted by investigators worldwide. It also examines, with reference to various laws, the legal position of an investigator when examining a mobile phone.

Key words: Mobile phones; SIM cards; Forensic investigation; ACPO guidelines

XFT – A Forensic Toolkit for the Original Xbox Game Console

David Collins
Department of Computer Science, Sam Houston State University,
P.O. Box 2090 Huntsville, Texas 77341
dcc002@shsu.edu

Abstract

The array of electronic storage devices is staggering in both number and type. The most common of these are IDE hard disk drives, laptop drives, thumb drives and other removable media like CD's and DVD's. Other media that are not as common but certainly as functional are high capacity magnetic card media, cell phones, PDA's, and game consoles. These devices provide a convenient means to store data of all kinds, but they also provide a way for criminals to possess and hide illegal material.

From a criminal's perspective, the original Xbox game console is a reasonable place to store and view illegal material such as child pornography. The original Xbox is not designed to support this activity, and because of this, it takes some modification to the operating environment to get this to work. Once an Xbox has been modified, it can be used to store and view illegal material. The Xbox uses the FATX file system. Aside from a few hacker web sites like xbox-linux.org, FATX is largely un-documented and is not readable by the leading forensic software; consequently, without an automated tool, a forensic examiner will have a difficult time getting information from a FATX file system, most likely resorting to a low-level analysis of a hex dump of the hard drives contents. Tools exist to extract files of a specific type in this fashion, however forensic browsing, searching, and organizing files in the file system is not feasible with this manual, low level approach.

XFT is a command line utility that will mount an image of a FATX file system as a logical drive, allowing full traversal of the directory structure. The XFT user interface is similar to a Linux shell. Once the Xbox file system is mounted, the analyst can use shell commands to browse the directory tree, open files, view files in hex editor mode, list the contents of the current directory in short or long mode, and expand the current directory to list all associated subdirectories and files. In addition, XFT will record a session to a log file so that the entire browsing session can be played back in a court of law. The tool is currently under development, and more functionality will follow including searching, sorting, recovery of deleted files, and smart file type recognition.

Digital Evidence Analysis in China

Zhijun Liu, Ning Wang, Yonghao Mai, Huanguo Zhang
Hubei University of Police; Wuhan University Computer School;
Key Laboratory of Computer Forensics, China

Abstract

Digital Evidence Analysis Phase is clear to supply sufficient information for the crime scenario reconstruction and suspected activity confirmation. Currently the data analysis phase is tedious, time-consuming, and requires significant expertise who owns very strong background knowledge. And an experienced investigator usually maintains a collection of search lists from his previous cases. In a new case, he could build the search list based on this collection or even re-use one from a similar case directly. So another problem is knowledge reuse. The investigator must handle digital evidences properly to guarantee integrity and reliability in Forensic investigative procedures. This paper discusses an operating procedure to analyze digital evidence by SanZhen Ministry of Justice, Hubei in China, there are limitations and deficiencies to current digital evidence analysis phase, such as Procedural, Technical, Social, Legal, etc in practice. To enhance the quality and reliability of digital evidence, we have built a framework which defines abstract representations of computer systems, digital evidence analysis procedures, and the type of cybercrime, and formalizes their relationship. Thus, given the information about a specific cybercrime, the model allows for the specification of a set of digital evidence analysis actions sufficient to identify the type of cybercrime. Alternatively, given a set of actions, the model allows for the identification of the type of cybercrime this set can detect. Considering the digital evidence analysis phase is manual and dependent on individual experience knowledge, we also consider Ontology Modelling for the above framework, the results of this paper can be used to improve digital evidence analysis in China.

Is Property Theft in Crime Investigation? Using OSS in Cybercrime Education

David Bennett and Paul Stephens
Canterbury Christ Church University
North Holmes Road, Canterbury, Kent CT1 1QU, UK

Abstract

Open Source Software (OSS) differs from much commercial software in that the source code is made available to users. Licensing arrangements for OSS normally means that it is available for free, and that it may be modified and used in a different project, but that any usage of it must remain open source. Examples of OSS are the Linux operating system and the office software suite OpenOffice.org (OpenOffice.org 2007). There is also OSS available that is useful for computer forensics investigations, such as The Sleuth Kit (sleuthkit.org 2007b) and Autopsy (sleuthkit.org 2007a). This paper critically reviews the potential for using OSS in educational and training courses. The paper will consider three main types of software – the Linux operating system, the use of open source utilities that are not directly linked to forensic investigations such as 'Disk Editor' (Shah, Mathews 2004)and the use of specific forensic software, such as Autopsy. Initially we distinguish between the uses of software in the workplace compared to those in educational settings. We then consider how arguments made for the use of OSS match up to the needs of education and training, in particular the arguments of Carrier (2003). The final section of the paper looks at the three types of software above. We base our commentary on three main areas:

- Quality of the software in general;
- Ability to discover concepts and theories in the field;
- Ability to move seamlessly into employment afterwards; and
- Cost and resource implications for educational establishments and forensic investigation teams.

In terms of quality, in generally we have found that most software is technically good. Where it seems to suffer is in the user interface and the user experience. Much as commercial software follows the development arc suggested by Norman (1998) in that user experience follows marketing and technical quality, we suggest that the same will happen in OSS. This is one aim of work by Bennett and Stephens (2008) in reviewing the usability of Autopsy. In terms of the ability to discover concepts and theories of the field, there are no major issues in the use of OSS, as the domain generates the language used by the software. We look at the impact of terminology; the effect of being able to view code and how this is affected by the prior knowledge expected of a student. The ability to move seamlessly into employment is an area that is mixed. We discuss the impact of the type of tool, its current utilisation in the workplace and the effect of moving from one software product to another. In terms of cost and resource implications for educational and forensic teams there are again a number of different factors, related to total cost of ownership, including initial purchase costs of software and equipment, the gaining of the required expertise by trainers and lecturers and long term maintenance and support. We then consider the cost implication to industry of retraining staff from one software system to another.

Understanding digital certificates

Mick O'Brien and George R S Weir
Department of Computer and Information Sciences,
University of Strathclyde
Glasgow G1 1XH
mickobrien137@hotmail.co.uk, george.weir@cis.strath.ac.uk

Abstract

Digital certificates are a core component in the provision of secure data communications. Gaining an understanding of the nature, creation and operation as well as the variety of these certificates is an essential step for students of computer, information or network security. In order to clarify the relationship between central technologies, including symmetric and asymmetric encryption, digital signatures, certificate key stores, certificate revocation lists, and the use of digital certificates in secure Web transactions, we have developed a software tool that allows users to explore these aspects of data security. This paper outlines some of the surrounding issues and describes the 'sandpit' application as a means of exploring and, thereby, gaining a better understanding of digital certificates.

The Social Effects of Spam

Man Qi, Raza Mousoli, Denis Edgar-Nevill
Department of Computing
Canterbury Christ Church University
Canterbury, UK
CT1 1QU
{man.qi, reza.mousoli, denis-edgar-nevill}@canterbury.ac.uk

Abstract

With the prevalence of the Internet and the development of e-commerce, e-mail has become the primary means of communications and marketing. However, the abuse of e-mail is pervasive in the mean time. Unsolicited electronic messages and commercial information, also called spam, impedes the Internet effectiveness to individuals and baffles the consumers' acceptance of e-marketing. It not only hinders the growth of the e-commerce but also causes severe social problems.

Bill Gates promised in 2004 that spam would have been solved in two years. As he left his job at Microsoft on 27th June this year, spam continues to its historical growth. Since 2006, with spam levels have steadily climbed from 56% to its present state of 80% of all email, the social threats of spam have become eminent.

The paper presents the motivations of spammers, the potential profits in spamming and the economical and psychological influences to the spammed. The social effects of spam will then be analysed in detail. The effects include challenges to fair trade, public morals, cybersecurity, personal data protection, property rights for e-mail recipients' and other concerns.

Virtual environments have a prominent role in securing your organization: Case Study on a DDoS attack

Righard Zwienenberg
Norman Data Defence Systems Ltd, UK

Abstract

Virtual Environments, whilst having been around for a number of years, are tipped to be the “next big thing”. Virtual technology and varying degrees of sandboxing are being incorporated in a growing number of mainstream products. Most virtual environments will run the original operating system or a modified version using systemhooks to keep control, however this is open to potential exploits within the operating system and so the control is compromised. The Norman SandBox Analyzer has its own operating system which simulates everything, including intranet and internet, if required. In addition the Analyzer can provide live connections to the internet where the resulting data is only applied in the safe simulated SandBox environment.

The execution of malicious code within a network environment can be costly, especially when it comes to the new and unknown threats that are increasingly targeting organizations.

This seminar will show how Norman utilize virtual technology to analyze suspicious file behaviour and will highlight a number of cases where Analyzer has proved successful in analyzing and minimizing the impact of security threats including a DDoS attack and DropZones.

During the seminar an attempt will be made to connect to a live botnet and if possible to the Command and Control centre of the botnet to show the way to analyze these botnets and the instructions the zombies receive.

Egregious use of Tor Servers?
Data retention, anonymity, and privacy on-line

F.W.J. van Geelkerken
Tilburg Institute for Law, Technology, and Society
Tilburg University, Montesquieu Building – M710
P.O. Box 90153, 5000 LE Tilburg, The Netherlands
F.W.J.vangeelkerken@uvt.nl
Tilburg Graduate Law School, Tilburg University
Montesquieu Building – M228, P.O. Box 90153
5000 LE Tilburg, The Netherlands

Abstract

This paper deals with data retention, which is defined as being any operation, or set of operations which is performed upon traffic and location data and the related data necessary to identify the subscriber or user, whether or not by automatic means, such as collection, recording, organization, storage, or retrieval.

First how the data retention directive (2006/24/EC) harmonises and regulates the retention of amongst other the traffic data of internet use is elaborated on. Based on article 5 of this directive data necessary to trace and identify the source and destination of a communication, data necessary to identify the date, time, duration and type of communication, and data necessary to identify users' communication equipment need to be retained.

Afterwards an elaboration why, through the harmonisation of data retention obligations on providers of public electronic communication networks, the detection, investigation and prosecution of serious crimes is made considerably easier, is given. As data retention can however also infringe on the right to privacy as formulated in article 8 of European Convention on Human Rights, an explanation is given how using onion routing, the technique employed by Tor, the objective of the data retention directive, easier detection, investigation and prosecution of serious crimes, can be made more difficult if not impossible.

Finally, four ways of regulating behaviour both off-line and on-line as formulated by Lessig are explained and grounds as to why Tor should, and why it should not, be legislated are given.

Comparison of Drupal and Joomla security functions for designing secure Content Management System

Raza Mousoli
Department of Computing
Canterbury Christ Church University, Canterbury, UK
CT1 1QU
reza.mousoli@canterbury.ac.uk

Abstract

Drupal and Joomla are currently two of the most popular Open Source PHP Content Management System (C.M.S) in the marketplace. This paper will evaluate and compare Drupal and Joomla technologies and their associated access control features and build-in security functions.

To have inbuilt and default security procedures and functions with a given system software makes the job of a system designer easier in terms of analysis, design and coding. In contrast, it makes hacking and attacking of the site much more difficult as the system is less vulnerable to security coding weaknesses. For a less experienced programmer in PHP this might become a daunting task and end up with a weak and unsecure design. JoomlaSecurity has been developed to address security issues and detect any intrusion, addition, deletion of the code on the root directory and the use of htaccess file that influences any request that is made to a site. On the other hand Drupal access setting and controls are powerful tools for vetting and authenticating users.

Drupal and Joomla have solid security features that enable a user to design secure systems and we will discuss good features within both systems. Although we will not carry any major testing of both systems, however we will review available technical documents and literature concerning PHP security features in Drupal and Joomla.

Case-oriented evidence mining in forensic computing: A case study

Jun Zhang [1,2], Lina Wang [1]
1. Department of Computer Science and Technology, Wuhan University, Wuhan 430072, Hubei, China
2. Department of Information Technology, Hubei College of Police, Wuhan 430034, Hubei, China,

Abstract

Digital forensic analysis is challenged by increasing variety and complexity of cases, mass volumes of data, and state-of-the-art technologies exploited by criminals or unscrupulous individuals. Investigators need experience, skills, and keen detective minds in conducting forensic sound examinations. However, what the most important is the practicable methodology to guide forensic performances. Many crime investigation models and processes have been presented so far, whereas in some situations when investigators faced with a large number of seized servers and laptops, they may be overwhelmed due to the lack of an obvious start point from which they begin with their very first steps.

In this paper, we proposed a new forensic investigation model, named COEM (case-oriented evidence mining model), along with its approaches, top-down. The model facilitates analysis through a viewpoint of case instead of data, and gives investigators a more natural and rational perspective. To illustrate the model, we also examined a digital crime case relating to the suspected distributing pornographic materials through WAP sites in China.

Evidence mining is a new term or, at least, scarcely used term. We use the term to refer to the application of data mining and knowledge discovery techniques to support the digital forensic investigations.

Section 1 of this paper describes the basic background needed in future discusses. Next, section 2 focus on the details of the new model and its approaches. This is followed by a discussion in section 3 of the case study. Concluding remarks and future works are provided in section 4.

Intrusion Forensics

Zeming Yang[1],Rongsheng Xu[1], Man Qi[2]
[1]Institute of High Energy Physics
Chinese Academy of Sciences
Beijing China
xurs@ihep.ac.cn
[2]Department of Computing
Canterbury Christ Church University
Canterbury, UK
man.qi@canterbruy.ac.uk

Abstract

The number of occurrences along with the severity of computer-based intrusions has become increasingly concerned. The digital intrusion forensics of this kind of events faces great challenges. In an attempt to better deal with these problems, this paper presents a case-based reasoning model for digital intrusion forensics. We have implemented this approach in our Digital Intrusion Forensics System (DIFS), which can analyse different sources of evidence automatically, correlate the evidence data, and conduct intelligent forensics using the knowledge learned from history cases.

Invited Keynote Presentation

“Digital Forensics Research in China”

Professor Rongsheng Xu
Network Security Group
Institute of High Energy Physics
Chinese Academy of Sciences, China

This speech will briefly review the status of computer forensics research in China since 2000, how the Committee of Experts on Computer Forensics (CECF) established technical research based on computer criminal and electronic data evidence, as well as who are the participants in CECF (China), and the seminars and basic reports in recent years in China. Some of research will be reviewed, such as, Modeling Computer Forensics Process (by Beijing Police College, Ministry of Public Security), Real-Time Forensic based on Operating System (by Institute of Software, CAS). As an example of forensic anti-Virus (Xiongmao Shaoxiang, Worm_Viking) will be introduced, which was the first case related to the spreading of computer viruses in China and the worm had hit millions of computers in the country since November 2006. The speaker will also review the status of training class of Digital Forensic in China, and with regard to China’s demand and International desirability of participation, the future of Digital Forensics technology and products exchange program in China will be discussed.

Introduction of Speaker

Professor at IHEP Computing Center, Beijing, China

- Deputy of Committee of Experts on Computer Forensic, China
- Working in Network Security since 1995
- Starting research on Computer Forensic since 2000
- Gave a Keynote Speech in Conference - HTCIA 2007 at San Diego, USA

Sponsor - Canterbury Christ Church University

The Department of Computing plays host to the CFET 2008 conference based at the North Holmes Road Campus of Canterbury Christ Church University.

The Department comprises of 10 full-time and 7 part-time staff running undergraduate an postgraduate courses for 300 students. The Department is centred in the Invicta Building of the North Holmes Road Campus which includes four purpose built computer laboratories with over 100 workstations.

The Department developed the MSc Cybercrime Forensics in 2004 which is jointly validated with the NPIA (National Policing Improvement Agency). This award is currently offered to serving police officers, members of High Tech Crime Units in the UK and other Home Office officials. In July 2007 the Department added an undergraduate award the BSc Forensic Computing to its course portfolio offered from September 2007.

In January 2007 the Department secured HEFCE funding for a two year project to promote the development of Cybercrime research in the awards both within the staff and students studying the subject. More details of this project are given later in this booklet.

Sponsor – National Policing Improvement Agency

The NPIA (formally CENTREX prior to 2007) provide specialist training and support to the 43 national police forces in the UK. NPIA will support the police service by providing expertise in areas as diverse as information and communications technology, support to information and intelligence sharing, core police processes, managing change and recruiting, developing and deploying people.

Their task is to help the police service take forward their priorities, working closely with the professional leadership of the programmes and services they are responsible for. In close co-ordination with our partners, ACPO, APA and the Home Office their role is to help face the challenging and demanding needs of policing in the 21st century

Sponsor – Justice Institute of British Columbia, Canada

JUSTICE INSTITUTE of BRITISH COLUMBIA

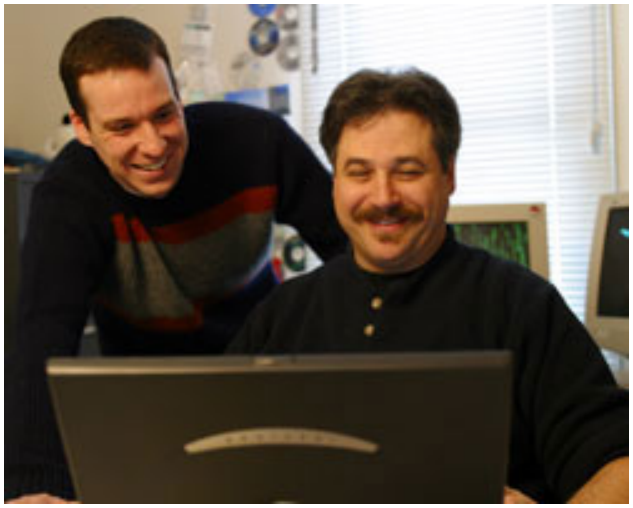
Provincial post-secondary institute, founded under College & Institute Act, for Justice & Public Safety education in 1978, by Dr. Patrick McGeer, Minister of Education. Its mission is to provide Innovative education and training for those who make communities safe. Its vision is to be a world leader in education, training and the development of professional standards of practice in justice, public safety and human services. Offerings include programs ranging from basic training to Bachelor degree programs. When it was founded in 1978 2,000 students were trained. Today, student numbers are over 30,000 annually, with more than 6,000 students in online programs. Instructors are in more than 190 communities in British Columbia delivering programs. In 2005/06, 6,249 organizations chose the Justice Institute of BC for training, education, and research needs in justice & public safety training.

Sponsor – Champlain College, USA

Founded in 1878, Champlain College is a private, baccalaureate institution that offers professionally focused programs balanced by a strong core curriculum. The College is a national leader in educating students to become skilled practitioners, effective professionals and global citizens.

Created in 2006, the Champlain College Centre for Digital Investigation (C3DI) has a charter to assist law enforcement agencies in Vermont and throughout the nation, particularly in areas related to computer forensics and other digital investigations. This goal is being achieved through a number of initiatives and partnerships between academia, the public sector, and the private sector.

The C3DI has been made possible by funding from the U.S. Department of Justice Bureau of Justice Assistance (BJA) and Champlain College, as well as material support from the Burlington Police Department and the Vermont Internet Crimes Task Force (ICTF).



Sponsor – Norman Data Defense Systems

Norman is one of the world's leading companies within the field of data security. With products for antivirus (virus control), personal firewall, anti-spam, and encryption, the company plays an important role in the data industry. Norman's products are focused on secure computing.

Products from Norman are available for both home users who want to surf the Internet and large corporations. And everyone in between.

Sponsor – Data DNA Ltd

Copyright Statement

Delegates List

(as of 18th August 2008)

Surname	First Name	Organisation	Country
Austin	Alan	Ipc Media	UK
Bennett	David	Canterbury Christ Church University	UK
Blundell	Bob	4Sight Forensics	UK
Brighouse	Brian	Canterbury Christ Church University	UK
Case	Nicola	Norman Data Defence Systems	UK
Childs	David	Digital Evidence Recovery & Internet Crime Lab	UK
Collins	David	Sam Huston University	USA
Davidson	Alan	Stockholm University and the Royal Institute of Technology	Sweden
Diemer	Henk	IBM	Netherlands
Edgar-Nevill	Denis	Canterbury Christ Church University	UK
Edgar-Nevill	Val	Canterbury Christ Church University	UK
Gay	James	Vocalink	UK
VanGeelkerken	FWJ	Tilburg Institute for Law, Technology, and Society	Netherlands
Gibson	Ed	Microsoft UK	UK
Gibson	Stuart	University of Kent	UK
Harley	David	Director of Malware Intelligence ESET LLC	UK
Henson	Richard	ESET LLC	UK
Hicks	Ryan	AVG Technologies	Czech Republic
Induruwa	Abhaya	Canterbury Christ Church University	UK
Jahankhani	Hamid	Middlesex University	UK
Jones	Nigel	University College Dublin/Risk Technology Ltd	UK
Kartiko	Iwan	Macquarie University	Australia
Kessler	Gary	Champlain College	USA
Koranteng	Kweku	University of Ghana	Ghana
Liu	Zhijun	Hubei University of Police	China
Marsh	Steven	University of Wales Institute Cardiff	UK
Mason	Steven	British Institute of International and Comparative Law	UK
Mousoli	Reza	Canterbury Christ Church University	UK
Norris-Jones	Lynne	Cardiff Metropolitan University	UK
Ohara	Toby	University of the West of England	UK
Oja	Rein	Stockholm University and the Royal Institute of Technology	Sweden
Overill	Richard	Kings College London	UK
Peteron	Chirsty	University of Glamorgan	UK
Phillips	Ruth	London Metropolitan Police	UK
Qi	Man	Canterbury Christ Church University	UK
Robinson	David	Norman Data Defence Systems	UK
Ross	Margaret	Southampton Solent University	UK
Stephens	Paul	Canterbury Christ Church University	UK
Stock	Gerald	Canterbury Christ Church University	UK
Thomas	Paula	University of Glamorgan	UK
Wakelin	Andy	University of Abertay	UK

Weir	George	University of Strathclyde	UK
Williams	Stephen	Data DNA Ltd	UK
Woodman	Suzie	National Policing Improvement Agency	UK
Xu	Rongsheng	Chinese Academy of Sciences Network Security Group	China
Zhang	Jun	Wuhan University	China
De Zoysa	Kasun	University of Colombo	Sri Lanka
Zwienenberg	Richard	Norman Data Defence Systems	UK

Maps of the Venue