CFET 2007

1st International Conference on Cybercrime Forensics Education & Training

Conference Programme & Abstracts

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

ISBN 1899253-041

Contents

Introduction to the Conference

Cybercrime Forensics one of the fastest areas of growth within Computing. This is a direct response to the growing complexity and vulnerability of computer systems and the new forms of criminal activities making use of them. The demand for people qualified to assist in cybercrime investigations is very large and growing. This has led to many universities world-wide offering undergraduate and postgraduate degrees in this new area.

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 and delegates from seven 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 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 first annual international conference and hope your stay with us is a very enjoyable and informative one.

Denis Edgar-Nevill
Chair, CFET 2007

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
Dr Abhaya Induruwa Canterbury Christ Church University
Paul Stephens Canterbury Christ Church University

International Advisory Panel
Susan Ballou
Program Manager, Office of Law Enforcement Standards, NIST, USA
Dr Robin Bryant
Head of Department (Crime & Policing)
Canterbury Christ Church University, UK
Dr. Joe Carthy
University College Dublin, Republic of Ireland
Dr Philip Craiger
Assistant Director for Digital Evidence, National Center for Forensic Science University of Central Florida, USA
Bill Crane
Acting Head of High Tech Training
National Centre for Policing Excellence - Specialist Training, UK
Dr. Rob D'Ovidio
Drexel University, USA
Denis Edgar-Nevill
Head of Department (Computing), Canterbury Christ Church University, UK
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, Aon Consulting, UK
Dr Gary C. Kessler
Director Center for Digital Investigation Information 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

Conference Schedule

Day 1 – 6th September 2007

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

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

10.45 - 11.45 **Plenary Presentation – Powell Lecture Theatre**
"High Tech Crime Training: A Model Outline
and How It Maps To Academic Programmes"
Bill Crane, Acting Head of High Technology Training
The National Policing Improvement Agency (NPIA), UK

11.45 - 12.45 **Parallel Presentation Sessions**

Cybercrime Education – Powell Lecture Theatre

"Integration of Computer Forensics into a Forensic Science programme"
Dr Richard E Overill, Kings College London, UK

"Cybercrime Training versus Computer Forensics Education"
Paul Stephens, Canterbury Christ Church University, UK

Computer Ethics – Powell Pg06 Lecture Theatre

"Should we be teaching computer ethics to computer forensics students?"
Alistair Irons, Northumbria University, UK

"Cybercrime: Is Computer Ethics a Weapon for Preventing Copyright Infringement?", WenHao Wang , Kate Dingley, Carl Adams
University of Portsmouth, UK

12.45 - 14.00 **Lunch**

14.00 - 15.00 **Plenary Presentation – Powell Lecture Theatre**
"Experiences and Methodologies Teaching Hands-On Cyberforensics Skills Online"
Gary Kessler, Director of the Center for Digital Investigation
Champlain College, USA

15.00 - 15.45 **Coffee & Exhibitors - Powel Foyer and Pg05**

15.45 – 16.45 **Parallel Presentation Sessions**

Cybercrime Education – Powell Lecture Theatre

"Cybercrime Forensics Experiences in a Developing Country"
Kasun De Zoysa, K S. Goonatillake, Kenneth M. Thilakarathna,
University of Colombo, Sri Lanka

"Research Informed Cybercrime Education"
Denis Edgar-Nevill
Canterbury Christ Church University, UK

Cybercrime Analysis – Powell Pg06 Lecture Theatre

"Analysis of and Extraction of Forensic Material from Malicious Code", Righard Zwienenberg, Norman Data Defence Systems, UK

"Pedagogy of Cryptology Education: A comparison of two groups"
David Bennett and Dave Lewis
Canterbury Christ Church University, UK

18.30 - 21.00 **Conference Dinner**

The Conference Dinner will be held in the Frederick Mason Room of the St Martin's Priory Campus of Canterbury Christ Church University, a 5 minute walk from the North Holmes Road Campus.

The Conference Dinner will include presentation of the Norman Data Defense Systems Prize.

Menu

Starters

Pork Terrine served with cornicons & chutney

(Vegetarian option - Tomato & Mozzarella Salad)

Main courses

Pork braised in oregano & lemon served with a timbale of mixed rice and an authentic Greek salad

(Vegetarian option - Roasted vegetable layers with toasted feta cheese)

Desserts

Chocolate Torte served with a berry sauce & cream

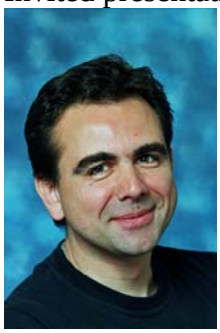
~~~

Coffee and Teas
~~~

Day 2 – 7th September 2007

09.00 - 10.00 **Plenary Presentation – Powell Lecture Theatre**

"RFIDIOts!!!– Practical RFID Hacking (Without Soldering Irons or Patent Attorneys) Adam Laurie
Invited presentation sponsored by The Bunker



10.00 - 10.45 **Coffee & Exhibitors - Powel Foyer and Powell Pg05**

10.45 - 12.45 **Parallel Presentation Sessions**

Cybercrime & Law Enforcement – Powell Lecture Theatre

"Prosecuting Low-level Cybercrime in the UK"
Clare Bracey, Sussex Constabulary, Denis Edgar-Nevill, Canterbury Christ Church University, UK

"A Critical (Legal) View of Forensic Computing"
Bernd Carsten Stahl, De Montfort University, UK

"Investigating the use of and the impact of mobile technology in gathering and manipulating data and digital images in tackling Fly-tipping in the Medway Towns"
Liz Faulkner & Dr Richard Henson
Canterbury Christ Church University, UK

Cybercrime Education – Powell Pg06 Lecture Theatre

"Footprints of Cyber Criminals"
Man Qi & Denis Edgar-Nevill
Canterbury Christ Church University, UK

"Virtual Reality and Interactive Training for Airport Security"
Manolya Kavakli, Macquarie University, Australia

"Human Trust and E-Trust"
Reza Mousoli, Canterbury Christ Church University, UK

"Managing the Pedagogy of Cybercrime Forensics Study at Post Graduate Level: Challenges and Opportunities"
Dr Abhaya Induruwa
Canterbury Christ Church University, UK

12.45 - 14.00 **Lunch**

14.00 - 14.30 **Plenary Presentation – Powell Lecture Theatre**
"Cybercrime Education and Training Virtual Forum"
Denis Edgar-Nevill, Canterbury Christ Church University

14.30 - 15.30 **Plenary Panel Session Powell Lecture Theatre**

15.30—16.00 **Coffee & Exhibitors**

1600 **Conference Close**

Presentation Abstracts – 6th September 2007

"High Tech Crime Training: A Model Outline
and How It Maps To Academic Programmes"
Bill Crane, Acting Head of High Technology Training
The National Policing Improvement Agency (NPIA), UK

"Integration of Computer Forensics into a Forensic Science programme"
Dr Richard E Overill
Kings College London, UK

"Cybercrime Training versus Computer Forensics Education"
Paul Stephens
Canterbury Christ Church University, UK

"Should we be teaching computer ethics to computer forensics students?"
Alistair Irons
Northumbria University, UK

"Cybercrime: Is Computer Ethics a Weapon for Preventing Copyright Infringement?"
WenHao Wang, Kate Dingley, Carl Adams
University of Portsmouth, UK

"Experiences and Methodologies Teaching Hands-On Cyberforensics Skills Online"
Gary Kessler
Director of the Center for Digital Investigation
Champlain College, USA

"Cybercrime Forensics Experiences in a Developing Country"
Kasun De Zoysa, K S. Goonatillake, Kenneth M. Thilakarathna,
University of Colombo, Sri Lanka

"Research Informed Cybercrime Education"
Denis Edgar-Nevill
Canterbury Christ Church University, UK

"Analysis of and Extraction of Forensic Material from Malicious Code"
Righard Zwienenberg
Norman Data Defence Systems, UK

"Pedagogy of Cryptology Education: A comparison of two groups"
David Bennett and Dave Lewis
Canterbury Christ Church University, UK

PLENARY PRESENTATION

"High Tech Crime Training: A Model Outline and How It Maps To Academic Programmes"

William N. Crane
Acting Head of High Technology Training
The National Policing Improvement Agency
Wyboston, Bedfordshire, England

Mr. Crane, a graduate of American University, Washington, DC, completed 30 years of U.S. Government service in January 1997, including 26 years in Federal law enforcement and 4 years in the United States Marine Corps. He began his law enforcement career in 1971 with the U.S. Immigration Service in California and also served as a Special Agent in Miami, Florida and Washington, D.C. He became a Supervisory Agent in Washington and soon after was selected as the first Special Agent to be assigned to the newly created Nazi War Crimes Unit in the U.S. Department of Justice.

In 1981 Mr. Crane was selected as the Deputy Director of Headquarters Operations at the Office of Inspector General, U.S. Department of Education. He held increasingly responsible positions in several Offices of Inspector General and, upon retirement, was the Deputy Assistant Inspector General for Investigations at the U.S. Department of State. Upon retirement from the government, Mr. Crane joined the National White Collar Crime Center in August 1997 and was promoted to Assistant Director, responsible for the Computer Crime Training Program, in the spring of 1998. As a collateral duty with NW3C, Mr. Crane served as Director of the National Cybercrime Training Partnership Operations Center. The NCTP was an international body of law-enforcement agencies, academia, and private sector companies involved in the development and delivery of high-technology training for the law enforcement community.

In 2005 Mr. Crane accepted a position with the National Centre for Policing Excellence (NCPE), in England. In April of 2007, NCPE was folded into a new agency, The National Policing Improvement Agency (NPIA). Mr. Crane has been Acting Head of the NPIA's High Tech Crime Training programme since July, 2006.

Mr. Crane became involved in computer crime in 1982. He has been a guest instructor at the U.S. Federal Law Enforcement Training Center's Seized Computer Evidence Recovery Specialist training program and The FBI Academy. He is certified by the International Association of Computer Investigative Specialists in the seizure and analysis of computer systems. He also holds an A+ technical certification from CompTIA,® Computer Technician and Windows Administrator certifications from Brainbench® and is certified as an Information Systems Forensic Investigator by the International Systems Forensics Association. He has been a guest instructor for IACIS and represented the U.S. Department of State at a number of domestic and international conferences on computer crime issues. Mr. Crane also served on a number of National Institute of Justice Technical Working Groups involved in the Forensic Sciences and Digital Evidence. While residing in West Virginia, he was an Adjunct Professor at Fairmont State College and is currently enrolled in a Master's Degree in Cybercrime Forensics programme at Canterbury Christ Church University in Canterbury, England.

Integration of Computer Forensics into a Forensic Science Programme

Dr Richard E Overill
Department of Computer Science
King's College London

Abstract

In 1985 King's College London initiated what was at that time the only UK MSc programme in Forensic Science. Initially coordinated by the Department of Biochemistry, and latterly by the Forensic Science and Drug Control Unit, this interdisciplinary MSc programme is supported by teaching contributions from a wide range of academic departments across the College, as well as by external expertise from such organisations as the Forensic Science Service and the Metropolitan Police.

From the very outset the Department of Computer Science was invited to contribute to the MSc in Forensic Science and over the past twenty-one years its contribution has evolved considerably in both content and extent, although the present author has remained the computer scientist responsible for this curriculum.

This paper traces the development of the Computer Forensics content of the MSc in Forensic Science at King's College London. It identifies the key interfaces between Computer Forensics and traditional Forensic Science, and analyses the rationale for the selection and development of the Computer Forensics curriculum within that context. Finally it evaluates the degree to which the integration of Computer Forensics into a Forensic Science programme has been successfully accomplished, using student feedback data and examination statistics collected over a twenty-one year period.

Cybercrime Training versus Computer Forensics Education

Paul Stephens
Department of Computing
Canterbury Christ Church University

Abstract

In 2002 under the European Commission (EC) funded Falcone Programme an expert group comprising law enforcement officials and academics from across the European Union held several meetings to identify areas for improvement in training for high tech crime investigators. Having examined the training programmes available in several member states the group concluded that a European approach to cybercrime training and education was required. The panel of experts recommended that university accredited training in computer forensics be provided to law enforcement officers that is consistent throughout the member states. Provision should be made for sharing of training materials and the development of new resources in an attempt to minimise workload and promote best practice [O Ciardhuain, S., Patel, A., and Gillen, P. 2003].

The following year several members of the Falcone Programme expert group secured funding from the EC to carry out these recommendations. The funding was made available through the AGIS Programme [AGIS 2003] under the title "Cybercrime Investigation – developing an international training programme for the future". As a direct result of this project Canterbury Christ Church University, along with several other higher education institutions, was invited to explore the possibility of working with the National Policing Improvement Agency (NPIA) [NPIA 2007] High Tech Crime Training Centre to extend and enhance their training provision to a Master's level qualification. The MSc in Cybercrime Forensics had its first intake in September 2004 [CCCU 2005] for which the author is a course leader for three of the modules.

In addition to the MSc, the author has been involved with the development and delivery of a number of computer forensics training and education courses. The Department of Crime and Policing Studies runs an ICT and Forensic Investigation module as part of its BSc in Forensic Investigation which the author taught on for the first time this academic year. The author helped to develop and was part of the training team for the AGIS 2006 pilot training course Linux as a Forensic Tool. CCCU's Department of Computing is also in the final stages of validating a BSc in Forensic Computing [CCCU 2006] for which the author is the Programme Director Designate and a major contributor to several of the modules.

This paper will discuss the major similarities and differences between the training provided by the NPIA and AGIS Programmes and the education provided by CCCU from the particular experience of the author as both a trainer and as a lecturer.

Bibliography

[AGIS 2003] European Union AGIS Programme 2003-2007 to help legal practitioners, law enforcement officials and representatives of victim assistance services from the EU Member States and Candidate Countries to set up Europe-wide networks, exchange information and best practices
http://ec.europa.eu/justice_home/funding/agis/funding_agis_en.htm

[CCCU 2005] "Canterbury Christ Church joins forces with central police training and development authority to deliver masters degree in cybercrime forensics", Canterbury Christ Church University website, 24th June 2005,
http://www.canterbury.ac.uk/news/newsRelease.asp?newsPk=517

[CCCU 2006] "New degree in Forensic Computing", Canterbury Christ Church University website, 4th October 2006,
http://www.canterbury.ac.uk/news/newsRelease.asp?newsPk=740

[NPIA 2007] National Policing Improvement Agency,
http://www.npia.police.uk/en/index.htm

[O Ciardhuain, S., Patel, A., and Gillen, P. 2003] "Training: Cyber Crime Investigation", International Federation for Information Processing (IFIP) website, 29th March 2007,
http://www.ifip.org/TESTIFIP/WebPages/openbiblio/opac/viewDocument.php?id=92&PHPSESSID=f11c46e158952626dca6ddad9b509c60

Should We Be Teaching Computer Ethics to Computer Forensics Students?

Alastair Irons
Northumbria University

Abstract

Introduction
The nature of computer forensics in dealing with cybercrime and computer misuse means the discipline often exists in an ethical 'grey area'. This is partly due to technology moving faster than legislation, and partly due to the changing circumstances of computer forensics investigations, taking place in a techno-legal environment without previous legal precedent. The continuously evolving technological environment, the opportunities afforded to cyber criminals, the 'development' of new cybercrimes and the fact that legislation often lags technology, suggest that computer forensics investigations often give rise to a series of new computer ethics issues. The objective of this paper is to explore the issues surrounding the teaching of computer ethics to computer forensics students, specifically at what point in the curriculum should this teaching take place, and what pedagogic methods should we employ. The paper will attempt to link the need for computer forensics ethics to the professional responsibilities of computer forensics practitioners, and the need to understand the legal environment for computer forensics investigations.

Should we be teaching computer ethics to computer forensics students?
There is debate as to whether computer ethics can be taught. It is argued that higher education courses can do little to address ethical concepts if the principles have not already been learned from other sources such as family, church or school. A counter argument proposes that ethics cannot be learned in most families, religious institutions or schools but instead must be taught as part of a formal higher education and professional syllabus. It is suggested in this paper that anyone delivering a Computer Forensics programme should embed and integrate ethical issues into the computer forensics curriculum and to ensure that this takes place, explicitly, from the beginning of the programme.

Are the ethical issues any different for computer forensics students?
It is argued in this paper that the ethical issues facing computer forensics students are different to those encountered by students on programmes in other computing disciplines. However, it is also suggested that computer forensics students also need to appreciate the wider computer ethics issues in addition to the specific computer forensics ethical issues.

Teaching computer ethics to computer forensics students requires raising the students' awareness of computer ethics issues, providing students with the underpinning ethical theory to understand the ethical implications of their actions and providing students with the tools to analyse and evaluate ethical dilemmas. In the domain of computer forensics this requires students to consider and understand the ethical implications in the analysis of computer forensics cases, in the use of computer forensics tools and in the application of computer forensics techniques, methods and procedures.

Students need to understand the ethical implications of their actions and decisions in any computer forensics investigation. The ethical approach taken in any computer investigation has the potential to have significant impact on the individual (victim, perpetrator and investigator) and potentially will have impact on society in general.

Conclusion

Computer ethics provides an interesting pedagogic challenge on computer forensics programmes. The full paper will provide discussion on the issues, an outline of successful practice and the development of a framework which will allow for computer ethics to be embedded into computer forensics programmes.

Cybercrime: Is Computer Ethics a Weapon for Preventing Copyright Infringement?

WenHao Wang, Kate Dingley, Carl Adams,
School of Computing
University of Portsmouth

Abstract

With the exponential development of Cyberspace, Cybercrime is rising rapidly and generating a vast number of serious impacts to the industry and individuals, particularly with regards to copyright infringements. This urgently requires more attention. While more advanced technologies and stronger law enforcement have been developed, none the less, the numbers of Cybercrimes are continuing to rise.

Computer Ethics, an important aspect of the professional development of Cyberspace, leads a very important role in preventing unethical behaviours such as Copyright Infringement. While ethics are essential, this report looks at a small survey, which indicates that unethical behaviour is more complex than supposed. There are multiple reasons behind cybercriminal behaviour, including cultural, technological and psychological explanations. An initial model is developed which captures some of the complexities in the relationship between ethical and technological limitations.

Technology can provide a level of prevention and protection; however, on its own it is insufficient to create a satisfactory level of protection. We have discovered in some cases, technology can even generate negative effects towards the good behaviours. This is important particularly while very limited law enforcements apply.

While technology is still not fully effective on its own, good ethical standards can be developed in order to minimise the potential threat of copyright infringements. Our results indicate that a fairly high proportion of computing students who have few technical difficulties in infringing copyright, should they choose to do so. The main reason for being unethical was appeared to be connected to individual motivation and inclination towards risky behaviour.

Copyright and Cybercrime issues are complex and are thuse likely to require multiple approaches. We conclude that the ethical solutions are more likely to succeed if they are underpinned by technology, and vice versa. Thus it is our contention that a high standard of ethical behaviour will be achieved and maintained by creating a culture of ethical standards. However, it is likely that the chances of successful maintenance of these standards will be improved by using technology to deter casual or exploratory infringements.

Experiences and Methodologies Teaching Hands-On Cyberforensics Skills Online

Gary C. Kessler
Champlain College
Burlington, Vermont, USA

Abstract

This paper describes some of the course design aspects of teaching computer forensics in an online environment. Although the focus of the paper is about online education at the undergraduate level, the basic premises are also applicable to graduate education and adult training. The paper will describe the need and rationale for the delivery of education and training in an online modality. In this context, online refers to asynchronous, virtual classrooms rather than self-paced or synchronous distance education. Virtual classrooms can provide an equivalent learning experience to a traditional classroom, complete with an instructor, fellow students, a course calendar, lectures, homework assignments, examinations, discussion threads, chat facilities, etc.; online classes can also achieve the same learning outcomes as their traditional counterparts. Online courses, particularly those that target adults, need to be designed with certain pedagogic models in mind; problem-based learning, collaborative learning, and constructivism are among those teaching and learning models that are most effective for adult learners and are well-supported by online course delivery.

Discussions about online education and training are quick to bring out the fact that the online modality is not appropriate for every instructor, every student, or every topic. The obvious question, then, is online coursework appropriate for learning the hands-on skills necessary for computer forensics and digital investigations? Our experience over the last three years suggests that the answer is a resounding yes. The paper presents a high-level overview of an online computer forensics curriculum and the overall design of online courses. A large part of this discussion will focus specifically on the design and content of an introductory and an advanced computer forensics course, with particular attention to multimedia technologies that add value in the online offerings, such as narrated graphical presentations and screen capture methods for demonstrating software. Several hands-on assignments, such as the analysis of drive or cell phone images, and the software that is employed to support those assignments will also be described.

Cybercrime Forensics Experiences in a Developing Country

Kasun De Zoysa*, K. S. Goonatillake†, Kenneth M. Thilakarathna‡
University of Colombo School of Computing
Colombo 7, Sri Lanka.

Email: *kasun@cmb.ac.lk, † ksg@ucsc.cmb.ac.lk, ‡ kenneth.tux@gmail.com

Abstract

At the heart of modern corporate crime and counterterrorism investigations, computer forensics is now the fastest growing segment of IT and law enforcement even in a developing country such as Sri Lanka. Law enforcement authorities in Sri Lanka sought help from the University of Colombo School of Computing (UCSC) as it is one of the main organizations responsible for computer forensic investigation in the country to investigate important court cases since year 2003. These cases vary from the incidents related to pornography to serious suspected terrorist activities. We used open source software on recovering and analyzing evidence to prove crimes in the courts of law. We uncovered the capabilities of open source software in an area which one may never thought of using it.

Research Informed Cybercrime Education

Denis Edgar-Nevill
Department of Computing
Canterbury Christ Church University

Abstract

Cybercrime Forensics is a new, undefined, discipline; emerging as a consequence of the rising tide of crime involving computers and responses from law enforcement agencies to combat it [EURIM 2004]. It draws upon a range of existing subject areas (law, computer systems, computer security) but also brings with it something new. It is not simply a case of "old wine in new bottles". Forensic computing began as the development of toolsets, formalising data recovery and analysis practice and the development of computer law. Attention has broadened to ethical, professional and social considerations as well as keeping pace with the increasing sophistication of technological advances of data gathering from mobile devices, from live systems and encryption. Much of the education in this remains at a skills level, and is focussed in the commercial sector and in law enforcement training centres. For the subject to move forward as an academic discipline it must be underpinned with a clear subject focus and research base.

This paper discusses the experience of the author in developing an MSc Cybercrime Forensics award [CCCU 2005] in partnership with the National Policing Improvement Agency (NPIA) [NPIA 2007] in 2004 and gives a progress report on a HEFCE funded Research Informed Teaching project [CRIT 2007] being conducted in association with students on that award and students on a new undergraduate award [CCCU 2006]. The study is to investigate how research in Cybercrime Forensics is developed in the academic team and in students as they study on the programme. Part of the development is to produce a knowledge base in this area to assist in identifying the boundaries of the subject and the current state of practice. This involves work with prominent researchers and educators in this field both nationally and internationally.

Reflection on practice and experience is of great importance in this applied discipline needing industry, law enforcement and universities to work together [AGIS 2003] [DFES 2004] [JENKINS et al 2005]. The paper goes onto consider the implications of the Leitch Report [Leitch 2006] more generally on skills development between industry and academia and how the work which has been done to date here may be a model for other organisations in building knowledge transfer bridges between practitioners and the university sector.

References

[AGIS 2003] European Union AGIS Programme 2003-2007 to help legal practitioners, law enforcement officials and representatives of victim assistance services from the EU Member States and Candidate Countries to set up Europe-wide networks, exchange information and best practices
http://ec.europa.eu/justice_home/funding/agis/funding_agis_en.htm

[CCCU 2005] “Canterbury Christ Church joins forces with central police training and development authority to deliver masters degree in cybercrime forensics”, Canterbury Christ Church University website, 24th June 2005, http://www.canterbury.ac.uk/news/newsRelease.asp?newsPk=517

[CCCU 2006] “New degree in Forensic Computing”, Canterbury Christ Church University website, 4th October 2006, http://www.canterbury.ac.uk/news/newsRelease.asp?newsPk=740

[CRIT 2007] “Cybercrime Education Informed by Research in a New Fast-Changing Discipline”, HEFCE funded Research Informed Teaching project blog http://cybercrimerit.blogspot.com/ Accessed May 2007

[DFES 2004] The Relationship Between Research and Teaching in Institutions of Higher Education, Department for Education and Science, UK Government, 2004, dfes.gov.uk/hegateway/uploads/Forum's_advice_to_Ministers_on_Teaching_and_Research...

[EURIM 2004] “Supplying the Skills for Justice: Addressing the needs of law enforcement and industry for investigatory and enforcement skills”, European Information Society Group (EURIM) third discussion paper, IPPR E-Crime Study drafted by UK MPs, 2004

[JENKINS et al 2005] Institutional Strategies to Link Teaching and Research, Jenkins A., & Healey M., Higher Education Academy, October 2005

[Leitch 2006] “Leitch Review of Skills: Prosperity for all in the Global Economy”, Final Report 2006, HMSO

[NPIA 2007] National Policing Improvement Agency (NPIA) http://www.npia.police.uk/, Accessed May 2007

Analysis of and Extraction of Forensic Material from Malicious Code

Righard Zwienenberg
Chief Research Officer
Norman Data Defense Systems Ltd

Abstract

The analysis of malicious code and the extraction of forensic material can be very time consuming. To do it properly, it can take days with the protection layers the nowadays malware uses to shield itself. In the past, the manual work was the only way to have a guaranteed result, but back then malicious code was tiny. Modern malware can be quite large, extremely protected, runtime compressed and runtime encrypted. The long days spent analyzing the code manually to extract the necessary information for forensic purposes will wear people down and errors will be made.

The use of automated tools to get quick and detailed analysis will help to improve the quality of this work. The Norman SandBox Analyzer products are a series of forensic utilities accomplishing exactly that by emulating the malicious code in a simulated environment. The malicious code can do its work affecting only the simulated environment and safely revealing its actions. All changes to the system (e.g. Registry, Services, File System, etc.) will be shown. In the most complex version of the Norman SandBox Analyzer, the user has full control of all actions as it includes full, 'real-time' debugging control of the simulated environment. Content created or altered on the virtual drive or virtual network storage, can be extracted into the real world for further analysis.

A lot of malware is nowadays internet-aware. Therefore the SandBox has the ability to connect to the real internet, where the actions happening as a result again will only affect the simulated environment. Having the SandBox connect to the real internet makes the analysis of botnets and botservers (the Command & Control centers) extremely safe and easy. Connections to these nets and servers are established upon the user's wishes and all information will be obtained. The botnet and botserver will not realize that the bot itself is running in a simulated environment.

During the presentation, several ways of extracting information will be demonstrated, from old methods to the new methods. Furthermore a connection to a botserver will be shown using one of the recently emerged botnets.

Alice Studies Computing, Bob takes Computer Forensics: A Comparison of the Pedagogy of Cryptology Education in Two Groups

David Bennett and Dave Lewis
Department of Computing
Canterbury Christ Church University

Abstract

Cryptology is an exciting area of computing to teach. Different audiences will have different goals in terms of their learning and the skills they need to take forward from a module in this area.

This paper compares two different cryptology modules taught to students on different programmes of study: those taking a BSc(Hons) in Computer Science and those taking a MSc in Cybercrime Forensics and discusses the issues raised. An overview of the differences between the courses is given in terms of their aims and objectives, structure, content, materials and books, tools and computer programs used, assessment modes and methods and links with other modules in the programme.

We conclude by discussing intended future changes to the modules and to the underlying programme that will have an impact on the two courses.

Presentation Abstracts – 7th September 2007

"RFIDIOts!!!– Practical RFID Hacking (Without Soldering
Irons or Patent Attorneys) Adam Laurie
Invited presentation
sponsored by The Bunker

"Prosecuting Low-level Cybercrime in the UK"
Clare Bracey
Sussex Constabulary
Denis Edgar-Nevill
Canterbury Christ Church University, UK

"A Critical (Legal) View of Forensic Computing"
Bernd Carsten Stahl
De Montfort University, UK

"Investigating the use of and the impact of mobile technology in gathering
and manipulating data and digital images in tackling Fly-tipping in the Medway Towns"
Liz Faulkner & Dr Richard Henson
Canterbury Christ Church University, UK

"Footprints of Cyber Criminals"
Man Qi & Denis Edgar-Nevill
Canterbury Christ Church University, UK

"Virtual Reality and Interactive Training for Airport Security"
Manolya Kavakli, Macquarie University, Australia

"Human Trust and E-Trust"
Reza Mousoli, Canterbury Christ Church University, UK

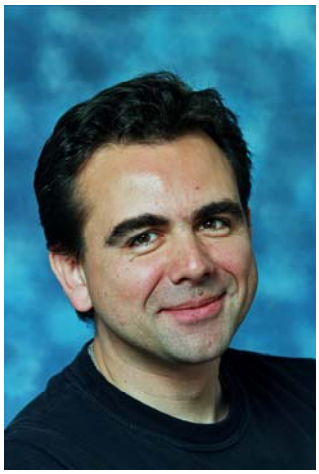
"Managing the Pedagogy of Cybercrime Forensics Study at Post Graduate Level:
Challenges and Opportunities"
Dr Abhaya Induruwa
Canterbury Christ Church University, UK

PLENARY PRESENTATION

“RFIDIOts!!!– Practical RFID Hacking (Without Soldering Irons or Patent Attorneys)

Abstract

RFID is being embedded in everything... From Passports to Pants. Door Keys to Credit Cards. Mobile Phones to Trash Cans. Pets to People even! For some reason these devices have become the solution to every new problem, and we can't seem to get enough of them... This talk will look at the underlying technology, what it's being used for, how it works and why it's sometimes a BadIdea(tm) to rely on it for secure applications, and, more worryingly, how this off-the-shelf technology can be used against itself... Software and Hardware tools and techniques will be discussed and demonstrated, and a range of exploits examined in detail.



Adam Laurie
Invited presentation
sponsored by The Bunker

Adam Laurie is a non-executive director of The Bunker Secure Hosting Ltd., and a freelance security consultant working the in the field of electronic communications.

He started in the computer industry in the late Seventies, working as a computer programmer on PDP-8 and other mini computers, and then on various Unix, Dos and CP/M based micro computers as they emerged in the Eighties. He quickly became interested in the underlying network and data protocols, and moved his attention to those areas and away from programming, starting a data conversion company which rapidly grew to become Europe's largest specialist in that field (A.L. downloading Services). During this period, he successfully disproved the industry lie that music CDs could not be read by computers, and, with help from his brother Ben, wrote the world's first CD ripper, 'CDGRAB'. At this point, he and Ben became interested in the newly emerging concept of 'The Internet', and were involved in various early open source projects, the most well

known of which is probably their own—'Apache-SSL'—which went on to become the de-facto standard secure web server.

Since the late Nineties they have focused their attention on security, and have been the authors of various papers exposing flaws in Internet services and/or software, as well as pioneering the concept of re-using military data centres (housed in underground nuclear bunkers - http://www.thebunker.net) as secure hosting facilities.

Adam has been a senior member of staff at DEFCON since 1997, and also acted as a member of staff during the early years of the Black Hat Briefings, and is a member of the Bluetooth SIG Security Experts Group and speaks regularly on the international conference circuit on matters concerning Bluetooth security.

He has also given presentations on forensics, magnetic stripe technology, InfraRed and RFID. He is the author and maintainer of the open source python RFID exploration library 'RFIDIOt', which can be found at http://rfidiot.org.

Prosecuting Low-level Cybercrime in the UK

Clare Bracey
Sussex Constabulary
Denis Edgar-Nevill
Canterbury Christ Church University

Abstract

The true levels of Cybercrime are difficult to estimate. The British Crime Survey [BCS 2007] does not include statistical information specifically in the area of computer related crime in its main body but does refer to criminal activity facilitated by computers, such as fraud, in associated reports [BCS 2004]. Financials organisations are reluctant to publish statistics in this area and may victims of such crimes also because the sums are small and there is a delay between deciding to purchase online and the expected receipt of goods weeks later [House of Lords 2006]. The numbers of offences are also hidden by the inability of individual forces to pursue investigations that involve perpetrators in other counties and Police Forces; especially for offences that individually involve small sums of money [ZDNet 2006].

In practice many Police Forces come across a large number of incidents of this kind. Some involve card not present fraud where goods are not despatched after purchase on online auction sites (such as eBay). Others relate to email offences that originate from another part of the country. In almost all cases the resources required to follow up investigations, to collect evidence and prosecute offenders, would far out weigh the sums of money involved in the original offence.

The need for a national recognition of this problem is discussed by the British Computer Society in their response [British Computer Society 2005] to a Home Office public consultation document [Home Office 2004]. The level of these offences fall far short of the national and international crimes investigated by SOCA (Serious Organised Crime Agency) [SOCA 2007] although Cybercrime is clearly an important part of their remit [Register 2007].

This paper gives the practical experience gained by the first author; as a serving police officer working in the High Tech Crime Unit of Sussex Police. It further goes onto propose a simple mechanism to allow for low-level crime not being taken forward for investigation to be at least signalled to other forces to help identify sudden increases in activity and clusters; pointing to activity within particular police force areas. The paper discussed the work forming the basis for a master's dissertation being completed by the first author in the area of Cybercrime Forensics [CCCU 2005].

References

[BCS 2007] British Crime Survey website
http://www.crimestatistics.org.uk/output/Page109.asp
(accessed 11th June 2007)

[British Computer Society 2005] Letter responding to public consultation document, January 2005, available at www.bcs.org/upload/pdf/crime.pdf (accessed 11th June 2007)

[CCCU 2005] "Canterbury Christ Church joins forces with central police training and development authority to deliver masters degree in cybercrime forensics", Canterbury Christ Church University website, 24th June 2005, available at http://www.canterbury.ac.uk/news/newsRelease.asp?newsPk=517 (accessed 11th June 2007)

[Home Office 2004] "Building Communities Beating Crime: a better police service for the 21st Centaury", available at www.homeoffice.gov.uk/documents/wp04_complete.pdf?view=Binary (accessed 11th June 2007)

[House of Lords 2006] "Personal Internet Security", Minutes of Evidence taken before the House of Lords Select Committee on Science and Technology, Wednesday 29th September 2006, available at http://www.parliament.uk/parliamentary_committees/lords_s_t_select/internet.cfm (accessed 11th June 2007)

[Register2007] "Cybercrime, Forget It!", Nigel Stanley, Bloor Research, The Register, 7th February 2007, available at http://www.theregister.co.uk/2007/02/07/untouchable_cybercriminals/ (accessed 11th June 2007)

[SOCA 2007] Serious Organised Crime Agency website http://www.soca.gov.uk/ (accessed 11th June 2007)

[ZDNet 2006] "Police will not pursue ransom hackers", ZDNet.co.uk, 2nd June 2006 available at http://news.zdnet.co.uk/security/0,1000000189,39272579,00.htm (accessed 11th June 2007)

A Critical (Legal) View of Forensic Computing

Bernd Carsten Stahl
De Montfort University, Leicester

Abstract

Forensic Computing (FC) is an emerging discipline located somewhere between computer science, information systems, legal studies and management studies. The apparent need for FC arises out of the increasing ubiquity of computers, which leads to computers being increasingly used in conventional crime but also the emergence of new computer-specific crimes. In order to teach the subject and to train and educate students and practitioners, it is imperative to have a strong understanding of its theoretical grounding. Much writing on FC, be it on its technical aspects or its ethical, legal and professional issues, comes from the positivist paradigm. This is problematic because FC, much more than other computing disciplines, is of a complex social nature.

This paper will thus chart a different course for the conceptualisation of FC. In the proposed paper I will chart a course for future critical research in FC. The theoretical references will come from critical theory of technology /critical research in information systems (CRIS) as well as critical legal studies (CLS). This comparison of several streams of critical research, all of which are pertinent for FC, is of interest because they represent very different stages of theoretical development. While CLS is an established discourse which has arguably peaked in the 1980s, CRIS is a relatively recent development. Analysing discourses in CLS can arguably help foresee and prepare for some debates still to come in CRIS.

Apart from this theoretical exploration, the paper will investigate the links between critical theory and FC. Using some of the traditional *topoi* of critical theory and critical research will help us better understand some of the recent developments in FC. The general public perception of FC is that it is an exact science which has the aim of supporting the conviction of dangerous criminals, including hackers and paedophiles. Critical theory can help question the assumptions on which this view is based and understand the mechanism used to project this view. The concept of ideology is helpful in showing how discourses on FC systematically favour some (large companies, intellectual property rights holders, technologically aware individuals) while they disadvantage others (adherents of deviant moralities, women, technophobes). FC, while recent in origin, is predominantly based on fundamentally conservative views. It is not only closely linked to capitalist means of reproduction but it uses a range of means for reproducing a conservative hegemony.

The paper will end by exploring ways in which these ideas can be put into research practice.

Investigating the Use of and the Impact of Mobile Technology in Gathering and Manipulating Data and Digital Images in Tackling Fly-tipping in the Medway Towns

Liz Faulkner & Dr Richard Henson
Canterbury Christ Church University

Abstract

For almost ten years now the government has been stepping up its efforts to tackle the problem of fly-tipping.

This paper outlines a case study and a prototype to use advances in mobile technology and Global Positioning Systems (GPS) to report and monitor incidences of fly-tipping in the field. Currently, Local Authorities and the Police rely on the public to report incidents of fly-tipping. This method of collecting and processing fly-tipping data is unstructured and imprecise making it difficult to identify hotspots and predict trends.

The case study delineates a prototype system to report fly-tipping via a Personal Digital Assistant (PDA). The PDA application records the location using GPS and can capture a digital image using an in-built camera. This data is then relayed to a central server via the internet.

Footprints of Cyber Criminals

Dr Man Qi & Denis Edgar-Nevill
Canterbury Christ Church University

Abstract

Cyber crime is changing as the Internet becomes a common communication platform and is a vital component of everyday life. Over the past few years, the number of cyber crimes has exploded. Given the technological nature of these crimes, some unique challenges are involved in tracking sources.

For instance, cyber criminals often use certain software to remain anonymous or falsify their identities. This paper starts with cyber crime cases to show their severe impacts and the value of traceability. There are also discussions on the characteristics of cyber crime: what it looks like, how it takes place, and how to fight it. Tracking footprints of cyber criminals is the first step and a key to the investigation. There are various types of electronic footprint which can be used, including telephone number, IP address, and router log, etc. The technologies using these identifications are reviewed here, which enable to find out the origination of a certain crime: in which country, which city, through which ISP, in which office or building and from which machine.

Currently a large number of tools are available to track the footprints of cyber criminals. This paper then discusses the difficulties in locating the footprints. The technologies being using to hide identities include using proxy servers, secure websites, or by routing communications through several different countries. Other high techniques can be using online anonymous servers and a vulnerable third party computer. There is also the likelihood of using falsified data. Cyber criminals are learning to play well with others, and that's bad news for the Internet. How to depict the footprint network is the new challenge for cyber crime fighting.

Virtual Reality and Interactive Training for Airport Security

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

Abstract

How can we secure a vast expanse of a country's border against criminal activity with limited human and capital resources? How can we train police officers in border security prior to taking over serious roles in border security? The objective of this project is to create an immersive virtual environment to support training of police officers using software tools for Crime Prevention Through Environmental Design (CPTED) and interacting with an airport model using multiple sensor modalities. Crime requires three components to occur: inclination, assets, and opportunity.

The goal of CPTED is reduction of criminal opportunity. This is achieved with physical design features that discourage crime, while encouraging legitimate use of the protected area. CPTED makes possible design solutions that offer protection without resorting to the prison camp approach to security. The task of an airport security program is to create an environment that lowers the comfort level of potential criminals, applying three principles: deter, delay, and detect. We 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) in our Virtual Reality Systems (VRS) Lab. VISOR consists of three projectors which display the virtual world onto a 6m wide semi-cylindrical screen canvas. The user is positioned slightly off centre towards the canvas to allow a 160° field of view. We use Vizard Virtual Reality Software, and speech and gesture recognition systems to interact with the objects at an airport. Our purpose is to test the effects of interaction on the quality of learning and to determine what factors are most important and pertinent to learning in an interactive virtual environment.

We will measure the effects of these factors in learning CPTED guidelines using a number of questionnaires. Integrated system, BOSS-CPTED, offers a prototype for testing the quality of learning in crime prevention specifically at the airports. In system development, to build the knowledge base, we have used a CPTED-SAC (Security Assessment Checklist) developed by Gardner (2002). CPTED-SAC is presented as series of yes or no questions. Questions are structured so that a positive response suggests the desired situation or condition. Each no indicates a possible weakness in the physical security program. As the learner eliminates the no answers, the level of protection increases. In this paper, we describe the system architecture of BOSS-CPTED, discussing crime prevention concept in general. BOSS-CPTED is composed of modules such as an Agent & Scenario-based Expert System, a Narrative Engine, a Game Engine, and a Graphics Engine.

Human Trust and e-Trust

Reza Mousoli
Department of Computing
Canterbury Christ Church University

Abstract

As the word “trust” derives from everyday English vocabulary, it has associated with it the usual vagueness and context dependency of a common language [1]. For the purpose of our research, firstly we will express the meaning of trust in relation to the fields of sociology, psychology, and human resource management. In relation to this, a model of trust will be discussed in details based on the notion of decomposition of the word trust into its basic ingredients; that is, we must first understand the nature of various types of trust and be able to deconstruct and synthesize it [2], [3].

Then we argue why these definitions of “trust” are abstract and not useful in computer science and why the new definition has to be concrete with known and measurable parameters and controllable outcomes [4]. In this context, i.e. computer security and resource allocation; security mechanisms are the means for implementing security services by means of prevention, detection and recovering valuable data; therefore the new definition should not be a subjective and arbitrary term. Hence we introduce e-trust and not trust as a quantity which has predictable qualities unlike human trust [5]. The computer industry’s interpretation and implementation of e-trust as expressed by major corporations and players in the computer industry such as IBM, HP and Microsoft are well established techniques. We argue why these implementations in the form of e-trusted sites and many trust management products are more of a marketing strategy or at best a binary resources allocation system that ignores credential based e-trust services [6].

We explore the use of logic of uncertainty, Bayesian logic, trust metrics and statistical techniques in providing a mathematical backbone to the construction of an intelligent e-trust management system [7], [8].

References

[1]D.H. McKnight and N.L. Chervany. What is Trust? A Conceptual Analysis and an Interdisciplinary Model. In Proceedings of the 2000 Americas Conference on Information Systems (AMCIS2000). AIS, Long Beach, CA, August 2000. MCC98

[2] Yi, Brian Corbitt, Theerasak Thanasankit, Trust on the world wide web: a study of consumer perception, School working paper series 2002/05

[3]Kini, A., and Choobineh, J. Trust in Electronic Commerce: Definition and Theoretical Considerations, Proceedings of the Thirty-Second Annual Hawai'I, International Conference on System Sciences, (Custom 2,1998)

[4] T. Grandison, M. Sloman, A survey of Trust in Internet Applications, IEEE 4th Quarter 2000

[5] Pauline Ratnasingham. The evolution of trust and electronic commerce security. Journal of Internet Security (published by ADDSecure.Net), 1(1), 1998.

[6] A. M. Chircu, G. B. Davis, and R. J. Kauffman. Trust, expertise and e-commerce intermediary adoption. In Proceedings of the 2000 Americas Conference on In-formation Systems (AMCIS2000). AIS, Long Beach, CA, August ,2000

[7] . Jøsang. A Subjective Metric of Authentication. In J. Quisquater et al., editors, Proceedings of ESORICS'98, Louvain-la-Neuve, Belgium, 1998. Springer

[8] B. Shand , J Bacon Policy in Accountable Contracts December 2001

Managing the Pedagogy of Cybercrime Forensics Study at Post Graduate Level: Challenges and Opportunities

Dr Abhaya Induruwa
Department of Computing
Canterbury Christ Church University

Abstract

In a 2003 report, the Westminster MPs stated that of more than 100,000 police officers in the UK only fewer than 1200 are trained to handle Cybercrime investigations. In 2005 the Canterbury Christ Church University launched an MSc programme representing an innovative partnership in higher education. This programme is designed to use the professional training modules offered by the High Tech Crime Unit of the National Policing Improvement Agency at Wyboston as a pre-qualifier and to impart a learning experience to the students at Masters level. The greatest opportunity offered by this partnership is to raise the level of academic achievement of those expert Cybercrime investigators working in the real world through University teaching, learning and research.

This paper examines the opportunities brought about by this partnership and the challenges faced in achieving its objectives.

Sponsor - Canterbury Christ Church University

The Department of Computing plays host to the CFET 2007 conference based at the North Holmes Road Campus of Canterbury Christ Church University.

The Department comprises of 12 full-time and 5 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 which will be 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

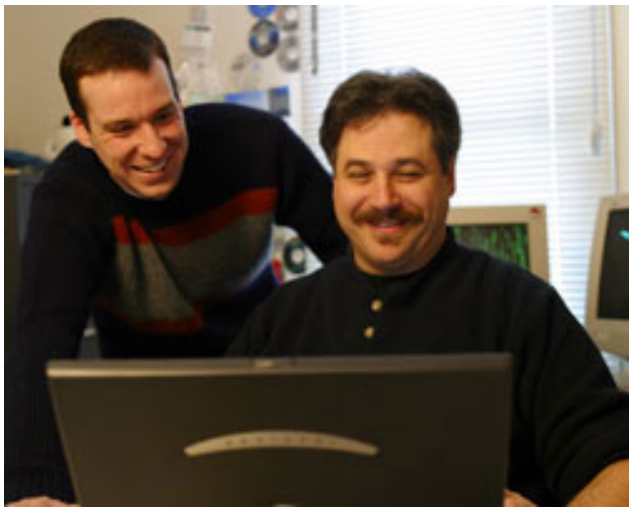
Provincial post-secondary institute, founded under College & Institute Act, for Justice & Public Safety education in 1978, by Dr. Patrick McGeer, Minister of Education. Its mission is to provide Innovative education and training for those who make communities safe. Its vision is to be a world leader 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.

Norman Data Defence Systems have offered a prize to one of the conference attendees in the form of a licence for 10 analysts using the Norman Online Analyzer (list price of £1250.00 + VAT). The prize will be presented at the CFET 2007 Conference Dinner on the 6th September 2007.

Sponsor – The Bunker

The Bunker provides Ultra* secure, ultra-available managed hosted and data centre solutions that ensure business continuity for the widest possible range of enterprises - from UK financial services giants such as Scottish Widows, to fast growing technology SME's such as ISB Ltd. Their solutions are delivered from 30 metres below ground level, from within armoured, military grade, nuclear proof facilities that are situated outside the perimeter of the M25. Each of them is based upon their unique security model - known as The Bunker Ultra* secure Shield - which addresses every potential physical, human and digital security threat.

HEFCE Funded Research Informed Teaching (RIT) Project

Cybercrime Education Informed by Research in a New Fast-Changing Discipline

The CFET 2007 conference is just part of a range of activities being developed by the Department of Computing as part of the wider RIT project. This development will study how research has informed the studies of students on the MSc Cybercrime Forensics and how this new area is being defined and developed by staff in the Department of Computing through the following activities:

- Developing a research network in Cybercrime Forensic including universities, police training NPIA and the National High Tech Crime Training Unit at Wyboston and commercial security companies promoting an annual international conference, developing an integrated website, virtual forums & streamed lectures using e-learning technology;

- One-to-one interviews with MSc students on the use of research informed teaching during the taught components of their programme and how this has influenced and developed their own research development;

- Interviews with prominent researchers in the field in the UK;

- Open research seminars with invited academics from other universities, police officers and security industry speakers;

- MSc students attending and present a research paper at the CFET 2007 international conference;

- Staff attending and presenting papers at CFET 2007;

- Staff research papers in the area of Cybercrime forensics and papers on RIT pedagogy.

In addition to a range of publications included in the CFET 2007 conference publications resulting from work on the project include:

> "Tracking Email Offenders", Man Qi & Denis Edgar-Nevill, ETHICOMP Working Conference 2007, Kunming, China, 2nd-3rd April, 2007
>
> "Using IT to Conduct Collaborative Research Across Distributed Staff & Student Populations" Denis Edgar-Nevill, CAQDAS2007 Advances in Qualitative Computing conference, Royal Holloway, University of London, 18th-20th April 2007
>
> "Motivating & Engaging Forensic Computing Practitioners in Higher Education", Denis Edgar-Nevill, accepted for Innovations in Lifelong Learning Conference, Birkbeck Institute for Lifelong Learning, Birkbeck – University of London, June 29th 2007
>
> "Work-Based Blended Learning through University Partnerships: A Case Study in Cybercrime Forensics", Denis Edgar-Nevill, abstract accepted for IERA2007 International Employment Relations Association 15th Annual Conference, Canterbury Christ Church University 8th-13th July 2007
>
> "Developing Cybercrime Forensics: The Growing Pains of a New Discipline", Denis Edgar-Nevill & Paul Stephens, accepted for the 3rd International Conference on Computer Science & Information Systems, Athens, Greece July 23-24 2007
>
> "Cybercrime Investigation Training and Specialist Education for the European Union", Paul Stephens & Abhaya Induruwa, accepted for 2nd Annual Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), Samos, Greece, 27-28 August 2007

Copies of any of the above publications are available upon request.

The project team welcomes any expressions of interest or willingness to co-operate or get involved with the project. Please contact:

Denis Edgar-Nevill
Head of Department, Department of Computing
Canterbury Christ Church University
North Holmes Rd, Canterbury, Kent CT1 1QU
United Kingdom
Tel +44 (0)1227 782089
Fax +44 (0)1227 782904
Email d.edgar-nevill@canterbury.ac.uk

Copyright Statement

Delegates List

(as of 1st August 2007)

Surname	First Name	Organisation	Country
Bennett	David	Canterbury Christ Church University	UK
Bowman	Kevin	Sheffield Hallam University	UK
Bracey	Claire	Sussex Constabulary	UK
Case	Nicola	Norman Data Defense Systems	UK
Chambers	Paul	Essex Police HTCU	UK
Crane	Bill	National Policing Improvement Agency	UK
Dawkins	Allan	Leeds Metropolitan University	UK
Edgar-Nevill	Denis	Canterbury Christ Church University	UK
Faulkner	Liz	Canterbury Christ Church University	UK
Ferguson	Ian	University of Strathclyde	UK
Goonatillake	Keerthi	University of Colombo	Sri Lanka
Induruwa	Abhaya	Canterbury Christ Church University	UK
Irons	Alistair	Northumbria University	UK
Jeffreys	Clive	Jeffreys & Associates, Solicitors	Austrailia
Kessler	Gary	Champlain College	USA
Kavakli	Manolya	Macquarie University	Austrailia
Laurie	Adam	Independent Consultant	UK
Lazarevski	Sanela	Leeds Metropolitan University	UK
Lewis	David	Canterbury Christ Church University	UK
Lightfoot	Paul	The Bunker	UK
Liyanage	Buddy	Independent Consultant	UK
Lloyd	Richard	cyfe-x.com	Nigeria
Marsh	Steve	Cardiff Metropolitan University	UK
McGee	Jack	Justice Institute of British Columbia	Canada
Milojcic	Neven	Independent Consultant	Croatia
Mousoli	Reza	Canterbury Christ Church University	UK
Nash	David	Essex Police - HTCU	UK
Neal	Simon	The Bunker	UK
Norris-Jones	Lynne	Cardiff Metropolitan University	UK
Ogujiofor	David	dandavies4us@yahoo.com	Nigeria
Overill	Richard	Kings College London	UK
Qi	Man	Canterbury Christ Church University	UK
Robinson	David	Norman Data Defense Systems	UK
Stahl	Bernd	De Montfort University	UK
Stephens	Paul	Canterbury Christ Church University	UK
Wang	WenHao	University of Portsmouth	UK
Wharram	Kevin	Sony Computer Entertainment Europe	UK
Williams	Stephen	Data DNA Ltd	UK
Woodman	Susan	National Policing Improvement Agency	UK
Zwienenberg	Richard	Norman Data Defense Systems	UK

Maps of the Venue