CFET 2011

5th 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
1st & 2nd September 2011

ISBN 978-1-899253-84-5

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 fifth annual international conference and hope your stay with us is a very enjoyable and informative one.

Denis Edgar-Nevill
Chair, CFET 2011

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 Man Qi Canterbury Christ Church University
Dr Abhaya Induruwa 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

Professor 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 former Head of Operations, National Digital Crime Investigations Unit, New Zealand

Dr. Rob D'Ovidio Drexel University, USA

Denis Edgar-Nevill Head of Department 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

Professor Nigel Jones Managing Director, Technology Risk Ltd, UK
Adjunct Professor University College Dublin, Republic of Ireland

Dr Manolya Kavakli Department of Computing, Macquarie University, Australia

Dr Gary C. Kessler Cybercrime Consultant, Vermont, USA

Jack McGee President, Justice Institute of British Columbia, Canada

Rob Risen Police Academy of the Netherlands

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

Professor Bill Buchanan School of Computing, Edinburgh Napier University, Director Centre for Distributed Computing

Dr Richard Overill Kings College London

CFET 2011 Conference Schedule

Day 1 –1st September 2011

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

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

Denis Edgar-Nevill, Chair CFET 2011
Head of Department Computing
Canterbury Christ Church University, UK

10.45 - 11.30 **Invited Keynote Presentation – Powell Lecture Theatre**
"Global Coordination and the Fight Against Cybercrime"
Introducing the International Cyber Security Protection Alliance (ICSPA)

Ian Sadler, ICSPA's Chief Administration Officer

11.30 – 13.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

11.30 – 12.15 ***"Formally Modelling Attack Patterns for Forensic Analysis"***
Clive Blackwell
Oxford Brookes University

12.15 – 13.00 ***"Man, Myth, Malware and Multiscanning"***
David Harley & Julio Canto
ESET North America

Powell Pg06 Lecture Theatre

11.30 – 12.15 ***"Automated Identification and Reconstruction of YouTube Video Access"***
Jonathan Patterson and Christopher Hargreaves
Cranfield University

12.15 – 13.00 **"Awareness and Training as the Key to Combating Cyber Crimes: by the Police force in the United Arab Emirates"**
Jasem Al Mansoori, Prof. Margaret Ross,
Dr Graham Benmore
Southampton Solent University

Workshop Computer Laboratory

11.30-13.00 ***"XRY Workshop"***
MSAB

13.00 - 14.00 **Lunch**

14.00 – 15.30 **Parallel Presentation Sessions**

Powell Lecture Theatre

14.00 – 14.45 ***"Forming a relationship between artefacts identified in thumbnail caches and the remaining data on a storage device."***
Sarah Morris, Howard Chivers
Cranfield University

14.45 – 15.30 ***"The Challenges of Live Data Forensics"***
Paul Stephens & Alastair Irons
Canterbury Christ Church University
& University of Sunderland

Powell Pg06 Lecture Theatre

14.00 – 14.45 ***"A Network Black Box with Splunk for Forensic Analysis"***
Clive Blackwell
Oxford Brookes University

14.45 – 15.30 ***"Multi-levels Privacy-Preserving Computer Forensics Investigation"***
Waleed Halboob, Muhammad Abulaish, Khaled S. Alghathbar
King Saud University, Saudi Arabia

Workshop Computer Laboratory

14.00 – 15.30 ***Cellebrite***
Miss. Adi Lutchinsky

15.30 - 16.00 **Coffee & Exhibitors - Powel Foyer and Powell Pg05**

16.00 - 17.30 **AGM BCS Cybercrime Forensics Specialist Group** (Open meeting)

16.00-16.15 Review of the last year
16.15-16.20 Committee Elections (BCS members only)
16.30-17.30 Invited Presentation
"Cyberforensics and International Police Collaboration: Trends and Challenges"

Dr Pavel Gladyshev
University College Dublin, Republic of Ireland

17.30 – 18.30 **BCS Cybercrime Forensics SG Committee Meeting** (Closed meeting)

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.

Day 2 – 2nd September 2011

09.00 – 10.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

09.00-09.30 ***"Cyber-Terrorism: A New Reign of Terror"***
Hemamali Tennakoon
Kingston University

09.30-10.00 ***"Cyber War"***
Denis Edgar-Nevill
Canterbury Christ Church University

Powell Pg06 Lecture Theatre

09.00-09.30 ***"DNS in Computer Forensics"***
Neil Fowler Wright
University of Westminster

09.30-10.00 ***Grid Computing for Large Scale Mobile Phone Analysis"***
Ed Day
Canterbury Christ Church University

Workshop Computer Laboratory

09.00-10.00 ***"The exploit, the exploiter, the exploited…"***
Righard J. Zwienenberg, Norman Data Defense Systems

10.00 – 10.30 **Coffee & Exhibitors - Powel Foyer and Powell Pg05**

10.30 – 11.15 **Invited Keynote Presentation – Powell Lecture Theatre**
"Creation of Dynamic Environments for Virtualised and Cloud-based Teaching in Digital Forensics and Computer Security"

Professor Bill Buchannan
Napier University

11.15 – 13.00 **Parallel Presentation Sessions**

Powell Lecture Theatre

11.15-11.50 ***"Cybercrime on VLEs (Virtual Learning Environments – Moodle, Blackboard, WebCT) visa vee the Social Networking and Single-Sign-On Insecurities"***
Robet Dube
Roehampton University

11.50-12.25 ***"Cyber Safety in Schools"***
Dr Man Qi
Canterbury Christ Church University

12.25-13.00 ***"The Virtual Tsunami: Global Disasters and Security Disasters"***
David Harley
CEO Small Blue-Green World

Powell Pg06 Lecture Theatre

11.15-12.00 ***"Digital Image Analysis for Evidence: A MATLAB Toolbox"***
Susan Welford and Dr Stuart Gibson
University of Kent

12.00-12.45 ***"Digital Astro-Forensics: the Final Frontier?"***
Richard E Overill and Jantje A M Silomon
King's College London

Workshop Computer Laboratory

11.30 – 13.00 ***Digital Detective***

13.00 - 14.00 **Lunch**

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

Professor Nigel Jones
Canterbury Christ Church University

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

15.30—16.00 **Coffee & Exhibitors**

1600 **Conference Close**

Presentation Abstracts – 1st September 2011

Invited Keynote Presentation

"Global Coordination and the Fight Against Cybercrime"

Introducing the
International Cyber Security Protection Alliance
(ICSPA)

Abstract

ICSPA) is a global not-for-profit organisation established to channel funding, expertise and assistance directly to assist law enforcement cybercrime units in both domestic and international markets. It is a business-led organisation comprising large national and multi-national companies who recognise the need to provide additional resourcing and support to law enforcement officers around the world, in their fight against cybercrime.

To ensure that it maximises the impact from its aims and objectives, the ICSPA will also seek resource and support from Governments and Institutions that understand the need to assist countries which face the greatest challenges and who wish to join in helping to combat all forms of cyber criminality. Furthermore, by increasing the capability, knowledge, training, skills, capacity and expertise of these front-line units, the ICSPA will have embarked upon a lasting strategy that will significantly help to reduce the harm caused to businesses, customers and citizens around the world.

This keynote presentation, by the ICSPA's Chief Administration Officer, Ian Sadler, will outline the aims and objectives of the organisation.

Biography

Ian Sadler has over 40 years police and security experience in both civil and military environments. After serving 16 years in the Royal Air Force, he held senior management positions in Banking and Retail security where he specialised in information assurance, business continuity and risk management. Ian is a Fellow of the Security Institute.

Formally Modelling Attack Patterns for Forensic Analysis

Clive Blackwell

Department of Computer Science
Oxford Brookes University
Oxford OX33 1HX. UK
CBlackwell@brookes.ac.uk

Information Security Group
Royal Holloway, University of London
Egham, Surrey. TW20 0EX. UK
C.Blackwell@rhul.ac.uk

Abstract

We have created a framework for modelling both forensics [i] and security [ii] that divides computer incidents into their various stages of access, use and effect. It also includes several sublevels of the logical computer layer including the application and network/OS layers. These aspects enable modelling incidents in their entirety, and it is possible to use the framework to formally model incidents in logic.

There is little work in formalising attack and forensic patterns to automate the creation of effective defensive measures and collection of incident data for subsequent investigation. The current informality of these patterns means that their utility is limited to manual use, so we extend the existing work [iii] on formalising design patterns, which would allow better reasoning about possible defensive response measures and subsequent forensic investigation. These attack and forensics patterns form a logical specification for the implemented defensive software to counter malicious attacks, and to collect adequate evidence for forensic analysis. This specification in logic, which is progressively refined into code, is a common method of developing high integrity software.

We could represent incidents using attack patterns[iv] from the Common Attack Pattern Enumeration and Classification (CAPEC) [vi], which are an extension of the widely used idea of design patterns [vii]. The elements of attack patterns are very similar to design patterns, except that they represent possible operational system misuse, rather than intentional designed functionality. We instead translate the OWASP (Open Web Application Security Project) top 10 most critical Web application security risks [viii]. This is easier, as OWASP use a simple framework to describe attack vectors that is a subset of our framework. We focus on the most important risks, because their remediation has greater impact, and it still demonstrates the value of formalising attack patterns.

The programs for detection and response to these attack or forensic patterns must be divided into components that can be implemented on network devices and hosts at both the network/operating system and application levels. Each field in the pattern needs annotation to aid its translation into programs at the various nodes with their differing recognition and response abilities. Our framework supports this by separately considering location, level, purpose, observation and power at each layer.

This possibly advances existing theory with realistic formal system modelling, because the analysis takes account of the goals and disposition of systems and the threats they face, rather than using some abstract and generic definition of security.

Bibliography

[i] C Blackwell, A Framework for Investigative Questioning in Incident Analysis and Response, *7th IFIP WG 11.9 International Conference on Digital Forensics*, Springer Advances in Digital Forensics VII, 2011.

[ii] C Blackwell, A Security Ontology for Incident Analysis, *6th Cyber Security and Information Intelligence Research Workshop*, ACM press, 2010.

[iii] Ian Bayley and Hong Zhu, Formalising Design Patterns in Predicate Logic, *5th IEEE International Conference on Software Engineering and Formal Methods*, 2007, pp 25-36.

[iv] Ian Bayley and Hong Zhu, Specifying Behavioural Features of Design Patterns in First Order Logic, *COMPSAC*, 2008, pp 203-210.

[v] Sean Barnum and Amit Sethi, *Introduction to Attack Patterns*, Cigital Inc, 2006, Build Security In, at https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/attack/585-BSI.html.

[vi] CAPEC, *Common Attack Pattern Enumeration and Classification (CAPEC)*, May 2011, at http://capec.mitre.org.

[vii] E Gamma, R Helm, R Johnson, and J Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley, 1995.

[viii] OWASP, *OWASP Top 10 -2010: The ten most critical Web application security risks*, OWASP (Open Web Application Security Project), 2010, at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Man, Myth, Malware and Multiscanning

David Harley
ESET North America
david.harley@eset.com
Julio Canto
Hispasec Sistemas Lab
jcanto@hispasec.com

Abstract

Malware multi-scanning: everybody's doing it. AV companies use batteries of competitor products for comparative analysis and other laboratory procedures. Blackhats are increasingly likely to use internal or third-party "black" laboratory resources for the testing of malware tweaked to increase resistance to anti-malware analysis and forensics, as the blackhat economy strengthens and parallels conventional business models. Public multi-scanner sites intended for the evaluation of the risk from individual files are also used and misused for many purposes, such as:

- Indirect distribution and gathering of samples
- The estimation and guesstimation of malware prevalence and of public exposure to risk from "undetected" malware
- The "ranking" of products by detection performance, and the subsequent generation of marketing collateral
- Pseudo-validation and classification of samples by testers.

Public sites have evolved and matured to meet the different needs of anti-malware vendors, a wide range of home and end users, other security researchers, and the media. However the range of myths and misconceptions around what is and isn't appropriate use has outpaced those developments. This paper and presentation will look at the history and range of multi-scanner usage in all these contexts, but will focus primarily on the inappropriate substitution of multi-scanning for (a) performance ranking and pseudo-testing, and (b) sound sample validation and classification.

This paper will consider five key points:

- Firstly, what's out there? We consider the multiplicity of public multi-scanner sites, in-house AV resources, specialist AV community resources and blackhat resources that are currently known to be in use as an anti-forensic measure.
- Secondly, we consider the sane and sensible uses for multi-scanning, including pre-validation sample processing, in-house comparative analysis, and risk assessment of individual files at public sites.
- Thirdly, we consider the misuse of public and private multiscanner facilities for pseudo-testing: is it a good idea to use multi-scanners for product ranking by detection performance?
- Fourthly, we look at pseudo-validation, addressing the issue of automation versus avoidance in sample validation and classification
- Finally, we address the implications for the anti-malware and product testing industries.

Automated Identification and Reconstruction of YouTube Video Access

Jonathan Patterson1, Christopher Hargreaves2
Centre for Forensic Computing
Cranfield University,
Shrivenham SN6 8LA, United Kingdom
1j.patterson@cranfield.ac.uk, 2c.j.hargreaves@cranfield.ac.uk

Abstract

YouTube is one of the most popular video-sharing websites on the Internet, allowing users to upload, view and share videos with other users all over the world. YouTube contains many different types of videos, from homemade sketches to instructional and educational tutorials, and therefore attracts a wide variety of users with different interests. The majority of YouTube visits are perfectly innocent, but there may be circumstances where YouTube video access is related to a digital investigation, e.g. viewing instructional videos on how to perform potentially unlawful actions or how to make unlawful articles.

When a user accesses a YouTube video through their browser, certain digital artefacts relating to that video access may be left on their system in a number of different locations. However, there has been very little research published in the area of YouTube video artefacts.

The paper discusses the identification of some of the artefacts that are left by the Internet Explorer web browser on a Windows system after accessing a YouTube video. The information that can be recovered from these artefacts can include the video ID, the video name and possibly a cached copy of the video itself. In addition to identifying the artefacts that are left, the paper also investigates how these artefacts can be brought together and analysed to infer specifics about the user‟s interaction with the YouTube website, for example whether the video was searched for or visited as a result of a suggestion after viewing a previous video.

The result of this research is a Python based prototype that will analyse a mounted disk image, automatically extract the artefacts related to YouTube visits and produce a report summarising the YouTube video accesses on a system.

Awareness and Training as the Key to Combating Cyber-Crime by the UAE Police Forces

Jasem Al Mansoori, Margaret Ross, Graham Benmore
Southampton Solent University
East Park Terrace, Southampton, Hampshire, United Kingdom
Jasem Al Mansoori jhfa123@hotmail.com
Graham.Benmore@solent.ac.uk Margaret.Ross@solent.ac.uk

Abstract

The paper discusses the content of training courses of the police force in the UAE, and their effectiveness. The results of a survey undertaken on the police training related to addressing the problems of cyber-crime in the UAE are evaluated.

The 222 respondents included all ranks that would be involved in combating or investigating cyber-crime, and included 70 officers and 148 other ranks. All police departments in the UAE were included, as well as the Police College in Abu Dhabi and the Communications Institute of the Ministry of the Interior. The educational level of the respondents was high; almost 40% had a degree. Just over 50% felt that that IT literacy was "sufficient ", but 8% felt that it was "low".

Sixty percent of respondents had some knowledge of cyber-crime. Sixteen percent of those had been given training relating to cyber-crime, and twenty percent had been involved in investigating or combating cyber-crime at work. Three of the respondents had received scholarships to study cyber-crime outside the UAE, on Master's degree courses. Twenty-six respondents had attended courses in cyber-crime investigation; most of which were held in the UAE. These included courses run by the Ministry of the Interior, the Police College, Zayed University, and the Sharjah and Dubai Police Forces. Nearly two-thirds of those respondents, who had attended these courses, felt that the course duration was too short.

Forming a Relationship Between Artefacts Identified in Thumbnail Caches and the Remaining Data on a Storage Device

Sarah Morris[1], Howard Chivers[2]
Centre for Forensic Computing, Cranfield University
Shrivenham, SN6 8LA, United Kingdom
[1]S.L.Morris@Cranfield.ac.uk
[2]H.Chivers@Cranfield.ac.uk

Abstract

The primary function of a thumbnail cache is similar between different operating systems; however there is no consistent implementation; because the thumbnails are potentially interesting to forensic analysts it is important to understand the detail of how they are used in a particular operating system. Previous work has shown the importance of understanding the structure and the effect of user behaviour on various thumbnail caches. However, an analyst needs to demonstrate a relationship between artefacts identified in the thumbnail cache and those found elsewhere on the system in order to provide context and corroboration of any evidence derived from thumbnails. A relationship between artefacts can also assist in establishing possible event time lines, and understanding the user behaviour which led to the system being in its current state.

This paper establishes the relationships which are formed between user generated files and information stored in the thumbnail cache; this shows how a forensic analyser can infer relationships between the thumbnail cache and other artefacts identified on the system. This paper provides a description of each relationship between the thumbnail cache and other artefacts; these relationships allow the corroboration of evidence extracted from the thumbnail cache and provide an addition source of evidence of user behaviour. In addition to providing a useful reference for analysts when reconstructing a user's activity, this paper also uses the thumbnail cache as an example to discuss the importance of contextual analysis within forensic computing.

The Challenges of Live Data Forensics

Paul Stephens
Department of Computing
Canterbury Christ Church University
paul.stephens@canterbury.ac.uk
Alastair Irons
Department of Computing, Engineering and Technology
University of Sunderland
alastair.irons@sunderland.ac.uk

Abstract

Traditional host-based forensics has favoured a 'pull-the-plug' approach to the acquisition, identification, evaluation, and presentation of evidence. Manufacturers of operating systems and software are making it increasingly easy for people to encrypt their data, making it difficult to retrieve this information without a password. Additionally, collection of server data or network data via host-based means can be difficult to justify. Encrypted data and enterprise data cannot therefore always be treated in the same way as traditional host-based approaches to computer forensics.

One solution is to harvest evidential materials from a live host. This approach, known as live data forensics, allows the collection of enterprise and encrypted data but it is not without its problems.

This paper explores the challenges of the live data forensics approach.

A Network Black Box with Splunk for Forensic Analysis

Clive Blackwell

Department of Computer Science	Information Security Group
School of Technology	Mathematics Department
Oxford Brookes University	Royal Holloway, University of London
OXFORD OX33 1HX. UK	Egham, Surrey. TW20 0EX. UK
CBlackwell@brookes.ac.uk	C.Blackwell@rhul.ac.uk

Abstract

We have developed the concept of forensically sound networks, where it may be possible to prove that certain computer incidents will either fail or otherwise collect sufficient data to determine their causality. We are building networks in common configurations in our labs to test them experimentally against different types of hacking and malware attacks. This can be checked by automatically generating large numbers of legitimate background network traffic with a packet generator, along with attack packets produced by penetration testing tools such as the Metasploit framework, and checking if the network meets its specification of allowing legitimate use whilst stopping undesirable incidents.

We use Splunk (the Google for machine data) for forensic analysis and incident response, as it is very adept at logging and merging data from multiple sources. Splunk can potentially collect the data needed to detect undesirable forensic patterns, whereas most current logging offerings, such as syslog used widely in UNIX, are inflexible and limited by collecting incomplete information in special formats, and lose information when translated into a lowest common denominator format such as syslog.

The practical implementation using Splunk has some similarities to a recent paper called 'Storage-Based Intrusion Detection' [1], which uses separate storage devices to monitor and report unauthorised or suspicious changes on host machines. Our logs are also kept separate from the machines they monitor, except we monitor networks rather than single hosts using a network black box on a separate control network.

The complete network is instrumented together with each host and its applications, with the logs merged to determine how and when the simulated incidents are caused, detected and responded to, along with their impact if successful. We intend to recreate, in a forensically secure manner, the cause, timeline, actions, progression and effects of each deployed network attack from the mass of collected network data. We note that our incident framework [2] structures incidents, amongst other things, into the main stages of access, use and effects, and into the various network layers, which helps systematic forensic analysis.

We collect, consolidate and analyse all the network traffic on a separate inaccessible control network for security. This can collect logging data from incidents that are difficult to stop such as the insider threat [3], which may allow us to establish accountability, because we have determined the relevant information required beforehand. We can also apply our idea to reactive security to stop or mitigate ongoing incidents, but this is hard, as automated response may cause more damage that it avoids.

References

[1] AG Pennington, JL Griffin, JS Bucy, JD Strunk and GR Ganger, "Storage-Based Intrusion Detection", ACM Transactions on Information and System Security, vol 13 no 4 (Dec 2010)

[2] C Blackwell, "A Framework for Investigative Questioning in Incident Analysis and Response", 7th Annual IFIP WG 11.9 International Conference on Digital Forensics, Springer Advances in Digital Forensics VII, 2011

[3] C Blackwell, "The Insider Threat: Combating the Enemy Within", IT Governance, 2009

Multi-Levels Privacy-Preserving Computer Forensics Investigation

Waleed Halboob, Muhammad Abulaish, Khaled S. Alghathbar
Center of Excellence in Information Assurance, King Saud University, Saudi Arabia
{wmohammed.c, mabulaish, kalghathbar}@ksu.edu.sa

Abstract

Computer forensics is an emerging field related to computer security which deals with extraction of digital evidence embedded within data stored on computer media. Although, a number of research efforts have been directed in this direction, privacy preservation is still open and challenging issue. In other words, privacy preserving and computer forensics are two opposite directions in computer security. The privacy preserving techniques try to protect privacy of users from any illegal disclosed, where the computer forensics tools try to discover all the user data, including data not related to the crime.

In this paper, we have proposed the design of a privacy-preserving computer forensics investigation process to make a balance between the computer forensics need and privacy preservation requirements. Different levels of privacy protection are defined and then a Privacy Preservation Engine (PPE) is proposed for preserving the defined user privacy levels - during investigation steps - while preserving the authenticity of collected digital evidence using an access control and audit trial mechanisms.

Keywords
Computer forensics; Privacy Levels, Evidence preservation; Digital investigation; Access control; Audit Trail.

Invited Presentation

Cyberforensics and International Police Collaboration: Trends and Challenges

Dr Pavel Gladyshev
University College Dublin, Republic of Ireland

Abstract

This talk will explore some of the current trends in the Information Technology and their impact on the ability of investigators to conduct Digital Forensics and Cybercrime investigations. The need for wider and more diverse training of law enforcement personnel dealing with cybercrime investigations will be highlighted as well as the importance of international collaboration between law enforcement, private sector and academia. In the second part of the talk, the issues impeding international collaboration against cybercrime will be discussed.

Biography

Dr. Pavel Gladyshev is a college lecturer at the UCD School of Computer Science and Informatics, where he is directing the GDip/MSc programme in Forensic Computing and Cybercrime Investigation - an international distance learning programme for the law enforcement officers specializing in cybercrime investigations.

Dr. Gladyshev's research interests are in the area of Information Security and Digital Forensics. His current work is focusing on logical foundations of digital forensic analysis and its applications to investigations of cybercrimes. Dr. Gladyshev serves on the editorial boards of the International Journal of Digital Evidence and the International Journal of Digital Crime and Forensics. In 2005-2009 Dr. Gladyshev served as an invited expert of the Irish delegation to the Interpol working party on IT Crime (Europe).

Presentation Abstracts – 2nd September 2011

Cyber-Terrorism: A New Reign of Terror

Hemamali Tennakoon
Department of Informatics and Operations Management, Kingston Business School,
Kingston University,
Kingston Hill, Kingston upon Thames, KT2 7LB, United Kingdom
K1014954@kingston.ac.uk

Abstract

The evolvement of the Internet and the dawn of the Web 2.0 has revolutionized the way in which individuals, groups and organisations interact. The novelty of Web 2.0 is in the way it empowers the users, giving them more control and ownership of data. Moreover, the emergence of social media, ubiquitous technologies such as smart phones, tabs and pads etc. has enabled users to communicate and interact with flexibility and ease. However, this heightened sense of freedom is beginning to threaten the lives of not only cyber dwellers but also those of innocent civilians. Imagine another 9/11, but this time an attack launched in cyber-space.

With the increasing dependence on Information Technology (IT), communication networks and systems, cyber-space has become the latest attraction for terrorist groups. It is the new weapon of mass destruction and an attack targeted at the critical systems of a country is enough to endanger the lives of millions of individuals. Internet and social media has becoming a breeding ground for cyber-terrorists because of the ease with which they could manipulate and exploit it for illicit activities. Therefore, cyber-terrorism, a controversial topic in the information society today is the focus of this brief paper.

The paper is structured around four main areas. First, the often-misinterpreted term of 'cyber-terrorism' is discussed in the context of terrorism studies. Secondly, the seriousness of cyber-terrorism is highlighted to emphasize on the importance of the issue at hand. It is useful to have an understanding of why and how cyber-terrorist attacks succeed in causing the intended damage on the target. While the third section of the paper focuses on this areas, the final section is dedicated to discussing possible remedies or strategies to minimize cyber-terrorist attacks. The nature of cyber- attacks are rapidly changing as the technologies change and new preventive/protective mechanisms need to developed in order to keep up with such changes. Some general solutions have been pointed out which are particularly applicable to today's organisations in protecting their information technology infrastructure from cyber-terrorist attacks. Furthermore, a practical framework has been suggested which can be adopted as part of organisational IT risk management practice. This framework is yet to be empirically tested, but there is indeed room for future where practical frameworks can be developed that are either more industry specific or ones that can be customised to suite the organisation in question.

Keywords
Information Technology, Cyber-terrorism, Risk, Management, Organisations

Cyberwar

Denis Edgar-Nevill
Chair BCS Cybercrime Forensics SG
Head of Department, Department of Computing
Canterbury Christ Church University
North Holmes Rd, Canterbury, Kent CT1 1QU, United Kingdom
denis.edgar-nevill@canterbury.ac.uk

Abstract

No one is quite sure about what a Cyberwar is. At what point do we stop talking about Cybercrime and start talking about Cyberwar? The explosion of news in December reporting the first great cyberwar unleashed as a consequence of perceived attacks on WikiLeaks has resulted in the term acquiring a new celebrity in thousands of column inches in news papers, website pages and hours of TV reports. It's almost as if we assume everyone understands the term.

This presentation will look at the development of the concept of Cyberwar and parallels with conventional warfare. It will discuss the technologies being used to wage war and the stages of events which can take place. Examples of groups engaged in these activities and their motivations together with the defences being mounted by governments and companies.

DNS in Computer Forensics

Neil Fowler Wright
University of Westminster

Abstract

The Domain Name Service (DNS) is a critical core component of the global Internet and integral to the majority of corporate intranets. It provides resolution services between the human-readable name-based system addresses and the machine operable Internet Protocol (IP) based addresses required for creating network level connections. Whilst structured as a globally dispersed resilient tree data structure, from the Global and Country Code Top Level Domains (gTLD/ccTLD) down to the individual site and system leaf nodes, it is highly resilient although vulnerable to various attacks, exploits and systematic failures.

This paper examines the history along with the rapid growth of DNS up to its current critical status. It then explores the often overlooked value of DNS query data; from packet traces, DNS cache data, and DNS logs, with its use in System Forensics and more frequently in Network Forensics, extrapolating examples and experiments that enhance knowledge.

Continuing on, it details the common attacks that can be used directly against the DNS systems and services, before following on with the malicious uses of DNS in direct system attacks, Distributed Denial of Service (DDoS), traditional Denial of Service (DOS) attacks, DNS cache poisoning and malware. It explores both cyber-criminal activities and cyber-warfare based attacks, and also extrapolates from a number of more recent attacks the possible methods for data exfiltration. It explores some of the potential analytical methodologies including; common uses in Intrusion Detection Systems (IDS), as well as infection and activity tracking in malware traffic analysis, and covers some of the associated methods around technology designed to defend against, mitigate, and/or manage these and other risks, plus the effect that ISP and nation states can have by direct manipulation of DNS queries and return traffic.

This paper also investigates potential behavioural analysis and time-lining, which can then be used for the development of automated analysis methods during forensic investigations and as DNS is a network protocol, there is a predomination towards network based attacks and discovery. It shows the breadth of possible attacks and the scope of investigative approaches that can be employed.

Overall it is an exploration of the area of DNS in Computer Forensics, additionally providing a foundation for educational exploration and further subject research: it concludes by bringing together all these aspects to support the importance of DNS analysis in Computer Forensics.

Grid Computing for Large-Scale Mobile Phone Analysis

Ed Day
Canterbury Christ Church University

Abstract

There is increasingly a need for distributing forensic digital processing (Richard & Roussev, 2004). So called "first generation" forensic tools such as EnCase and FTK were limited in both automation of tasks, and their ability to exploit parallel processing (Ayers, 2009), although FTK, for example, now has distributed processing capabilities. FTK allows for the uses of multiple processing workers (a worker can have more than one processor itself), and 4 workers can handle a 75GB PC image in 2.75 hours (AccessData, unknown). This image size is comparable to current smartphone storage sizes: a maximum 64GB on an SD card, with the next generation rumoured to support 128 GB, so we might expect similar timescales for phone analyses. AccessData in partnership with Dell also claim even more enhanced processing speeds but this is utilizing a "data centre" with "high performance servers," (Dell, 2009).

Grid computing provides a very powerful (parallel) computing resource; in essence this type of computing links resources ("nodes") in a "grid" by allowing a user to run a program that uses vast distributed resources that are situated and maintained remotely. The grid allows a number of nodes to process the data in parallel thus providing substantial time benefits. There are many such computing grids, for example the FBI has an internal grid computing network, the Grid Computing Initiative which utilizes unused capacity from their users' PCs (FBI, 2010). The National Grid Service (NGS) is another such computing grid and has been used for a number of research applications where massive computing power is needed, for example to model criminal behaviour of individuals within a city (Malleson et al, 2009).

I propose to use distributed grid computing techniques to be able to analyse multiple mobile phone images in parallel. One particular application occurs in major investigations when multiple phones related to multiple suspects are found, and the police would like to use the phones to prove associations between the suspects. Obviously if gang member A's phone has called Gang member B's phone this is somewhat straight forward, but an ideal solution would be an automated process that searches in more depth on the phones for any shared data, perhaps matching keywords in a text message. Existing software such as I2's Analyst's Notebook can provide a partial picture of associations and such software is fine when analysing a couple of phones but when more phones are handled the time taken to compare these phones increases significantly. Even for a manageable number of phones I2 has limitations for example it cannot handle raw image files requiring instead input from software such as EnCase (I2, 2011).

In the proposed method each of the grid nodes would receive the multiple mobile phone images. One node might handle searching and matching for photographic images another for SMS another for video and so on. Since each node is performing its particular search/match at the same time (in parallel with others) the time taken for all searches/matches is simply the time for the longest search/match. If the searching/matching was not done in parallel the time taken would be the sum of all the searches/matches. The matching algorithm will ideally allow flexibility in defining what constitutes a match.

References

AccessData. Unknown. Distributed Processing. Available from: http://accessdata.com/distributed-processing [viewed July 18th 2011].1

Ayers, D. 2009, "A second generation computer forensic analysis system", Digital Investigation, vol. 6, pp. 34-42

Dell., 2009. Dell Transforms how Police Analyse Digital Evidence with Digital Forensics Solution. Available from:http://content.dell.com/uk/en/corp/d/press-releases/2009-07-07-digital-forensic-uk.aspx [viewed July 18th 2011]

FBI., 2010. On the Grid: Computers Crunch Numbers in their Sleep. Available from:http://www.fbi.gov/news/stories/2010/january/grid_012210/on-the-grid-computers-crunch-numbers-in-their-sleep

I2, 2011, "Analyst's Notebook", http://www.i2group.com/uk/products--services/analysis-product-line/analysts-notebook, Last accessed 08/06/2011

Malleson, N., Evans, A. & Jenkins, T. 2009, "An agent-based model of burglary", Environment and Planning B: Planning and Design, vol. 36, no. 6, pp. 1103-1123.
Roussev, V. & Richard III, G.G. 2004, "Breaking the performance wall: The case for distributed digital forensics", Proceedings of the 2004 digital forensics research workshop (DFRWS 2004).

Workshop Computer Laboratory

The Exploit, the Exploiter, the Exploited…

Righard J. Zwienenberg
Chief Research Officer,
Norman Data Defense Systems,
righard.zwienenberg@norman.com

Abstract

As long as there have been computer systems, vulnerabilities exist and have been exploited. There are people that have made it their business to find vulnerabilities and there are people that have made it their business to 'use' the vulnerabilities. And you have people that do both. And as well, their motives are as diverse. What kind of companies are keeping themselves busy looking for exploits, what kind of people are (mis)using them. What are they looking for, what are they after? The presentation will deal with this going back to the early nineties to very recent events. Will we ever resolve the problem of exploits, being the exploited? Or be the exploiter?

Invited Keynote Presentation

Creation of Dynamic Environments for Virtualised and Cloud-based Teaching in Digital Forensics and Computer Security

Professor Bill Buchannan
Napier University

Abstract

The use of virtualised and cloud-based environments provides an excellent opportunity to enhance learning and to provide students with skills which match exactly to the requirements of industry, along with integrating with professional certification. This presentation shows two examples, in computer security and digital forensics, where students can learn on enhanced infrastructure which would not have been possible before the extensive development of virtualised and cloud-based infrastructures. This has been applied in both undergraduate and postgraduate programmes, along with teaching of advanced methods digital forensics and security to law enforcement professionals.

It shows how a range of virtualised environments, including using Amazon Web Services, a university-built cloud, and from a UK-based cloud provider have been used to provide exposure to a wide range of environments which are pre-build, or which are built-up throughout the module, and thus supports the students within a safe environment in which they can learn without any danger, and where errors can be easily undone. The environments can thus be created to use industry-standard tools and infrastructure, and these can be joined together to create collaborative work, along with the continuation of work after the practical lab work has been done.

The presentation shows the results from surveys of students on the module, and their perceptions of working within virtualised environments, and highlights that one of the key factors is that they can work in real-life and complete environments, and on a range of systems, which are well matched to the needs of industry. The presentation also shows how virtualisation has been used to support both blended and distance learning students using the same labs which are accessed within a face-to-face practical session, but done through a virtualised environment, all through a Web browser.

Finally, the presentation will present a new community cloud which allows students to work within a virtualised infrastructure (hosted by a UK company), and which industry and the public sector are able to contribute to in order to share training material and create relevant infrastructures for students.

Biography

Bill Buchanan is a Professor in the School of Computing at Edinburgh Napier University, and a Fellow of the BCS and the IET. He currently leads the Centre for Distributed Computing, Networks, and Security, and works in the areas of security, next generation user interfaces, Web-based infrastructures, e-Crime, intrusion detection systems, digital forensics, e-Health, mobile computing, agent-based systems, and simulation. Bill has one of the most extensive academic sites in the World, and is involved in many areas of novel research and teaching in computing. He has published over 27 academic books, and over 120 academic research papers, along with awards for excellence in knowledge transfer, and for teaching, such as winning at the I ♥ my Tutor Awards (Student voted), Edinburgh Napier University, 2011, and has supervised many award winning student projects.

Presently he is working with a range of industrial/domain partners, including with the Scottish Police, health care professionals and the FSA. As part of the drive to create a World-leading infrastructure for security and cybercrime, he leads the Scottish Centre of Excellence for Security and Cybercrime which bring together a wide range of collaborators, including most of the universities in Scotland, the Scottish Police, the public sector, and a range of SMEs and large organisations.

He has a long track record in commercialisation activities, including being a co-founder of Inquisitive System, which has progressed from PhD work to a university spin-out. This spin-out has also involved patenting novel digital forensics security software in three countries around the World. His current work includes a collaboration with Microsoft plc on a £2million project which aims to improve the care of the elderly using Trusted Cloud-based services, and with Chelsea and Westminster Hospital on a next generation Health Care platform. This also matches up with other funded projects with the FSA and the Scottish Police.

Cybercrime on VLEs
(Virtual Learning Environments – Moodle, Blackboard, WebCT)
visa vee the
Social Networking and Single-Sign-On Insecurities

Robet Dube
Roehampton University Business School
Roehampton University
80 Roehampton Lane, London SW15 5SL, United Kingdom
r.dube@roehampton.ac.uk

Abstract

I am at the early stages of my research into the security problems poised by the Social Networks to our Virtual Learning Environments (VLEs), particularly Moodle, Blackboard and WebCT. This is in regards to the now predominantly industry adopted technology of Single-Sign-On being implemented at corporate level for access to most corporate services, coupled with the ever increasing deluge of phishing of passwords and spam mail.

I am hoping to present some findings that l have collected thus far, as well as have an EXTENSIBLE DEBATE about what the delegates think is the next big challenge facing accessing our virtual learning environment.

The main focus of the paper and discussion/debate will be Privacy, Phishing, Single-Sign-On as well as the ever increasing use of VLEs at a time when universities are trying to raise money by focusing on long distance delivery of both undergraduate and postgraduate courses in times of austerity measures and the £9,000.00 fees.

Keywords
VLEs, Virtual Learning Environment, Phishing, Spam mail, Security, Single-Sign-On, One-Time-Codes, PINSentry, Social Networking, Moodle, Blackboard, WebCT, Facebook, Twitter, Bebo, MySpace, Ethics, Forensic, computers, investigation, privacy, law, legal, policing, Human Rights, Rights, Culture, custom, terror, terrorism, society, conspiracy, trust, religion.

Cyber Safety in Schools: Issues and Countermeasures

Man Qi
Department of Computing
Canterbury Christ Church University
North Holmes Rd, Canterbury, Kent CT1 1QU, United Kingdom
man.qi@canterbury.ac.uk

Abstract

The use of the Internet can greatly enhance the education and life experience of children in schools. As a new space in which children can learn and play, the Internet opens a world of possibilities to expand children's horizons, boost their creativity and provide opportunities to participate in society. According to recent research, 75% of 6-17 year olds in the EU-25 used the Internet in 2008.

However, the new space also exposes children to various risks. With the popularity of Web 2.0, where the Internet users can provide the information, upload photos and videos, blog, chat and join social networking, children easily become the victims of cybercrimes or engage in illegal behaviour themselves. The main concerns include giving out their private details, seeing pornography, violent or hateful content online, grooming for sexual abuse and cyber bullying.

Online grooming is one of the most serious issues to school children. Internet affords 'groomers' to contact children in anonymity, building up a relationship with them (pretending to be their friends) but only for the purpose of persuading children into sexual activity. Chat rooms and social networking sites are common platforms for this purpose. Various techniques have been used and there is increasing number of online grooming cases in recent years.

Cyber bullying and abusive postings on websites are another common and unfortunate by product of social networking services and open forums. It involves the use of the Internet to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others. In the UK, a reported 22% of children and young people claim to have been the target of cyber bullying. Cyber bullying is bringing bulling to a new extreme. Although it may not be of the physical kind, it is an extreme form of mental bullying, which can lead to stress, anxiety, depression or even suicide.

As these issues-related activities are considered as crimes, relevant laws would be powerful weapons to tackle the issues. In UK, there are no specific Acts for the particular issues. Some general laws as Sexual Offences Act 2003, Indecency with Children Act 1960, Protection from Harassment Act 1997, Malicious Communications Act 1988, and Communications Act 2003 are the main relevant piece of legislation. The legislation framework is lagging and inadequate. Other policies and countermeasures are necessary. Schools need to inform children about the online risks and how to deal with these risks. It is important to empower children to use the internet in a safe and responsible manner. It is also important for schools to establish public/private partnership to promote online safety measures.

The paper is to explore the typical online safety issues, present case studies, discuss relevant laws and other measures to protect safety of children in schools. The new

challenges to schools with the increased interactivity and mobility of web technology will also be explored.

References

[1] Nancy E. Willard, Cyber-safe Kids, Cyber-savvy Teens. Jossey Bass, 2007

[2] Ted Hastings, Internet Safety Skills, Leckie & Leckie, 2007

[3] Samuel C. McQuade, James P. Colt, Nancy B. B. Meyer, Cyber Bullying: Protecting Kids and Adults from Online Bullies Praeger Publishers Inc, 2009

[4] i-SAFE Internet Safety Activities, John Wiley and Sons, 2010

[5] Sonia Livingstone and Magdalena Bober, UK Children Go Online, Available from: www.children-goonline. net, 2005

[6] Chldnet International, Cyberbullying, Crown Copyright 2009

[7] Education on Online Safety in Schools in Europe, Education, Audiovisual and Culture Executive Agency, 2010.

[8] Vernon Jones and Ethel Quayle, Protecting Children from Online Sexual Exploitation. 2005, Available at http://www.childoscope.net/2009/httpdocs/publications/cddea67ce2be65c6c725b6513e782bcf.pdf (Accessed: 28th May 2011)

[9] Legislation.gov.uk, Available at http://www.legislation.gov.uk/ (Accessed 4th June 2011)

[10] Robin M. Kowalski , Susan P. Limber , Cyber Bullying: Bullying in the Digital Age, Wiley-Blackwell 2007

The Virtual Tsunami:
Global Disasters and Security Disasters

David Harley CITP FBCS CISSP
CEO, Small Blue-Green World
ESET Senior Research Fellow
David.harley@eset.com

Abstract

There's something about a disaster (global or personal, real or fabricated) that brings out both the best and the worst in people. While much of the world is eager to lend its support to afflicted regions, another eager subset of (in)humanity is taking to its keyboards, looking forward to profiting from the misery of others in a variety of ways: from fraud to malware, from spam to Black Hat Search Engine Optimization (BHSEO), from product misrepresentation to out and out hoaxes.

This presentation considers the evolution and classification of some of the species of maggot that emerge in times of tragedy to feed off the misery of those affected, and to profit (financially or otherwise) from the curiosity and sympathy of others. It looks at the ways in which we currently try to counter this exploitation, both within the anti-malware industry and outside it. And finally, we consider whether the cooperative models explored in other security contexts can be applied successfully to disaster management, or whether there's a way of doing it better.

The presentation is divided roughly into the following segments:

1. Phish and Foul Play: Charity/aid scams and spams, 419s, Londoning and ID theft, the evolution and divergence of misinformation and hoaxes;

2. Technical attacks, social engineering, and anti-social engineering: BHSEO, fake AV and other malware, and the misuse of social media and the escalating interconnectivity of social data;

3. What's been did and what's been hid: successes and mistakes in post-disaster security management: is there a more effective, more holistic approach to cybercrime and cybernuisance management during and following disasters?

Digital Image Analysis for Evidence: A MATLAB Toolbox

Susan Welford, Dr. Stuart Gibson, Andrew Payne
Forensic Imaging Group
University of Kent
Canterbury, Kent CT2 7NZ, United Kingdom

Abstract

In the last decade, affordable digital camera technology has become widely available, resulting in the proliferation of digital images. The creation, modification and distribution of certain photographic materials is controlled by law in the UK and in many other countries. For example, the production and possession of pornographic images of under 18s is prohibited in the UK by the Protection of Children Act 1978. It is similarly an o_ense to produce, modify and distribute any image that would be considered useful to a person committing, or preparing to commit, an act of terrorism under the Counter-Terrorism Act 2008. Digital image forensics is the science of determining the source of digital images and detecting the presence of image tampering (e.g. photo forgery).

The majority of research in this area has been conducted in the last decade by a small number of experts in the field of digital image processing. An understanding of these methods requires in-depth knowledge of image processing algorithms which most researchers and educators in the broader field of computer forensics do not possess. In this paper we describe our Digital Image Analysis for Evidence (DIAnE) toolbox, written in the MATLAB programming language.

Our approach is to utilises the inherent imperfections in image sensors that has previously been shown to produce consistent and unique noise patterns. The toolbox contains code libraries for generating device ‘fingerprints' that enable evidential images to be matched to their source cameras and graphical plots to facilitate easy understanding of the resulting correlation data. We believe DIAnE to be the only available MATLAB toolbox that performs this role.

Digital Cosmo-Forensics: the Final Frontier?

Richard E Overill and Jantje A M Silomon
Department of Informatics, King's College London
Strand, London WC2R 2LS, United Kingdom
{richard.overill | jantje.a.silomon}@kcl.ac.uk

Abstract

In this paper we study the likelihood that digital forensic evidential traces could be corrupted or otherwise compromised by extra-terrestrial physical processes and their epiphenomena. Specifically, we consider cosmic rays with solar, galactic and extra-galactic origins. The potential of such cosmic rays or radiation to alter the individual bits of current memory devices (hard disc ferromagnetic grains, conventional CMOS RAM and SSD Flash memory) is investigated using scaling and statistical techniques. Our memory model for this study permits the incorporation of error correcting codes (ECC) such as Hamming single error correction, double error detection (SEC-DED) logic. The available data enables a quantitative determination of a strong upper bound on the frequency (or probability) of such potentially evidence compromising, naturally occurring events to be made. The relevance of our findings for proactively blocking a number of potentially mountable legal defence stratagems is discussed in the context of both *in vivo* and *post mortem* digital forensics.

Invited Keynote Presentation

Professor Nigel Jones MBE FBCS
Canterbury Christ Church University

Biography

Nigel Jones is currently a director of Technology Risk Limited, a company specialising in technology risk solutions and training and for 1st September 2011 he has been appointed as a Visiting Professor at Canterbury Christ Church University. He was most recently European Practice Leader and Managing Director of the Financial and Litigation Consulting Services Practice of a major insurance broker. Prior to this he was responsible for the creation of the National High Tech Crime Training Centre at the National Centre for Policing Excellence at Wyboston in the UK and was responsible for the creation of the design and delivery of a core curriculum and modular high tech crime training programme for the UK police service. In addition to wide ranging experience in major commercial fraud and computer crime investigation, he was the Secretary of the Association of Chief Police Officers Computer Crime Working Group and the UK Internet Crime Forum as well as being the UK Police representative on the G8 sub group on high tech crime and UK coordinator of a series of G8 Industry conferences. During his time as a fraud investigator he designed and delivered an academically accredited fraud training programme.

Nigel formed the Kent Police Computer Crime Unit in 1993 and is co-author of the ACPO "Computer Based Evidence - Good Practice Guide" and member of the Technical Working Group on the Investigation of Electronic Evidence (TWGIEE) in the USA. In 2002 he was appointed by the UK as a member of the Interpol European Working Party on IT Crime.

In May 2009, he was invited to Interpol as an expert to provide advice on an international IT forensics investigation. He also chaired the cybercrime panel at the 2009 Interpol General Assembly. He is currently a member of the Home Office Forensic Regulators digital forensics specialist group which is assisting in identifying requirements for new or improved quality standards, applying to the provision of digital forensics services to the police service and the wider Criminal Justice System. Nigel is currently the training manager for a €2.7m European Commission funded programme to further harmonise cybercrime training across international borders. He is also the law enforcement coordinator for the creation of the international network of centres of cybercrime training, research and education (2CENTRE), funded by the European Commission.

Sponsor - Canterbury Christ Church University

The Department of Computing plays host to the CFET 2011 conference based at the North Holmes Road Campus of Canterbury Christ Church University.

The Department comprises of 10 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 offered from September 2007.

In 2008 as a result of CFET 2008 Denis Edgar-Nevill (Head of Department) was invited to propose the creation of the BCS Cybercrime Forensics Specialist Group which held its inaugural meeting at the University in December 2008.

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 – Cellebrite

About Cellebrite

Founded in 1999 by a team of highly experienced telecom and mobile telephony professionals, Cellebrite is a global company known for its technological breakthroughs in the cellular industry.

Wireless Retailers

The pioneers in mobile phone to phone content transfer, today Cellebrite provides a complete range of solutions for the mobile retail industry, from stand-alone content transfer at the POS to OTA applications for subscriber content management.

With proven ability to impact sales of phones, upgrades, and services, Cellebrite customers include the world's largest mobile operators and deployments by more than 140 major carriers.

Mobile Forensics

Building on its expertise in mobile data technology, in 2007, Cellebrite introduced a new line of products targeted to the mobile forensics industry.

Cellebrite's solution enables extraction and analysis of evidentiary data from more than 3,000 mobile phones and GPS devices.

The most complete mobile forensics experience available on the market today, Cellebrite technology is in use by military, law enforcement, and government agencies across the world.

Cellebrite is a fully-owned subsidiary of the Sun Corporation, a listed Japanese company (6736/JQ).

http://www.cellebrite.com/

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 – RTL

Modern day crime requires modern day policing and the increase of cyber crime means that police forces across the world need to be armed with the latest mobile forensic technology. Radio Tactics and its range of forensic solutions are equipped for this very occurrence.

Interaction with the community and crime deterrents remain hugely important parts of modern day local policing. In an effort to reduce and tackle every day crime, Radio Tactics has created a range of product solutions that offer the police everything from complete forensic analysis kits for the custody suites to truly portable devices ideal for on the street policing.

Sponsor – MicroSystemation

About Us

Micro Systemation (MSAB) is the global leader in forensic technology for mobile device examination, with offices in Europe and in the USA, as well as a network of distributors across the globe. The company has been involved with mobile communications since the 80's and now has a singular focus on the forensic recovery of data from mobile devices.

Our XRY software has been used by investigators to quickly and effectively retrieve information, such as pictures, SMS, call history, contact lists and application data since 2003.

XRY is used by Police, Law Enforcement, Military, Government Intelligence Agencies and Forensic Laboratories in over 60 countries worldwide to investigate crime, gather intelligence, investigate fraud and fight corruption.

In the UK alone we supply 95% of UK Police Forces with XRY for mobile device examination.

Micro Systemation's sole focus is a quality forensic solution that creates secure and trusted results for end users. The core business today produces a world class product called XRY which has the capability to recover deleted data from mobile devices; smart-phones, mobile phones, 3G modems, GPS and Tablet devices.

The company is based in Stockholm and has been listed on the Swedish Stock Exchange since 1999. We have been recognized by The Deloitte Technology Fast 500 EMEA program as a technology company that has achieved the fastest rates of annual revenue growth in EMEA during the past five years.

Awards and recognition received for the company include:

- Di Gasell Company (Swedish)
- AAA (credit rate)
- Superföretag (super company)
- Deloitte Technology fast 50 (Sweden)
- Deloitte Technology fast 500 EMEA 2010

We enjoy a privileged relationship with our clients and it is our intention to keep it that way by listening to user feedback and constantly improving our solutions to meet future requirements.

http://www.msab.com/

Sponsor – The Carphone Warehouse

Overview

Carphone Warehouse Group plc (CPW Group plc) comprises a 50 per cent interest in the Best Buy Europe Group and a 47.1 per cent interest in Virgin Mobile France. CPW Group plc is actively involved in the management of these businesses through regular participation in operational and strategic meetings as well as board representation. However, it should be noted that CPW Group plc does not exercise overall control over either of these businesses at board or shareholder level – although in respect of both businesses, its consent is required for decisions which materially impact their strategic direction. CPW Group plc also has Carphone Property – a portfolio currently comprising four freehold properties – and a number of minority investments.

- The Best Buy Europe Group is a leading European retailer of mobile and other wireless technology and services. It operates c.2,430 stores in nine European countries, principally under "The Carphone Warehouse" and "The Phone House" brands. This business is evolving its existing retail proposition to provide a broader range of products and services associated with the "Connected World" through its 'Wireless World' format. During April 2010 it opened its first "Best Buy"-branded "Big Box" store format and later that year its online proposition, offering consumer electronics products and services. There are currently 10 stores. The Best Buy Europe Group also benefits from a profit sharing agreement with Best Buy Mobile, Best Buy's specialist mobile business in the US, which currently operates through c.200 standalone stores and dedicated Best Buy Mobile centres in all of Best Buy's c.1,100 stores.

- Virgin Mobile France is the fourth largest mobile operator in France, with 1.9 million customers, operating as an MVNO under the "Virgin Mobile" brand. The Virgin group also has a 47.1 per cent interest in the business, with the remaining 5.8 per cent. held by Financom S.A.S. and employees of the company.

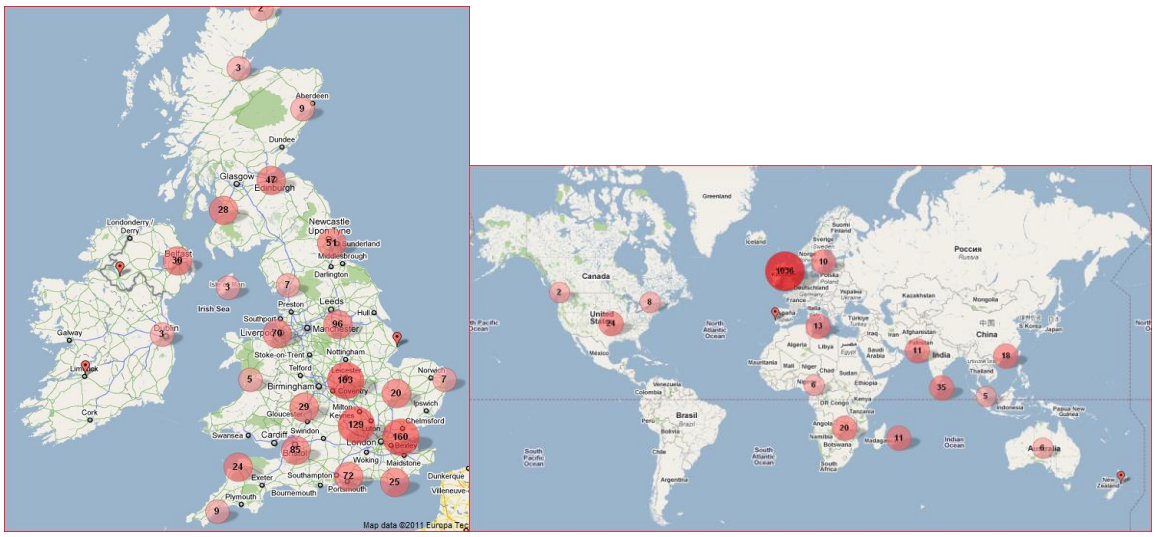
- Carphone Property currently comprises four properties in London, Manchester and Lancashire, with an aggregate book value of £68 million

http://www.cpwplc.com/

Sponsor – British Computer Society
Cybercrime Forensics Specialist Group

Cybercrime Forensics Specialist Group

Established in 2008, the SG now has over 1400 members in 44 countries:



Aim

"Promoting Cybercrime Forensics and the use of Cybercrime Forensics; of relevance to computing professionals, lawyers, law enforcement officers, academics and those interested in the use of Cybercrime Forensics and the need to address cybercrime for the benefit of those groups and of the wider public."

http://www.bcs.org/

Sponsor – Data Detective

Digital Detective first came into being in 2001 and has been providing quality software, resources and support to the worldwide digital forensic community ever since. The Forensic Forum now has in excess of 5,000 users and is a valuable resource for Digital Forensics, Mobile Phone Forensics and Digital CCTV Forensics. Our forensic software has in excess of 7,500 users worldwide.

In 2002, Digital Detective released NetAnalysis, a software product designed specifically for the forensic computing community, for the extraction and analysis of internet trace evidence. This software is in use by law enforcement agencies and companies worldwide and comes with a comprehensive manual detailing evidence extraction and analysis techniques.

Since its release, this software has become more advanced and now offers the examiner greater functionality when it comes to extracting and analysing Internet trace evidence. The software also has an extractor for recovering Internet history from image files, binary dumps and write protected drives and images. It was the first forensic software to recover deleted Internet trace data and the first to rebuild pages from the cache. It is the industry leader for the forensic analysis of browser trace evidence.

Internet History Extraction & Analysis: NetAnalysis

Forensic Data Recovery & Analysis: Blade Professional

Forensic Browser History/Cache Recovery: HstEx

http://www.digital-detective.co.uk/

Copyright Statement