CFET 2014

7th International Conference on
Cybercrime Forensics Education & Training

Conference Programme
&
Abstracts

Canterbury Christ Church University
Faculty of Social & Applied Sciences
Department of Law and Criminal Justice Studies
Centre for Cybercrime Forensics
North Holmes Road Campus
Ramsey Building
10th & 11th July 2014

ISBN 97801909067158

Contents

Introduction to the Conference

The 7th International Conference on Cybercrime Forensics Education and Training CFET 2014 is being held at an exciting time for the subject of Computer Forensics which is developing rapidly in a number of different directions in many countries around the World.

As a meeting place for those interested in this field it has in part led to the creation of a number of EU funded projects. In particular The ECENTRE project is funded by the European Commission under the ISEC programme. CFET 2014 is the main dissemination event for the project which includes extensive cybercrime training, software tool development, building a repository of educational materials and new research as part of the wider network of European Commission funded centres of excellence. The development of the project was discussed and facilitated by the CFET conferences since 2010 and has brought together many groups in the UK and beyond.

We have to in particular thank the European Commission's Directorate General Home Affairs for sponsoring places for law enforcement in the UK and from across the EU at this years' conference – and we extend a warm welcome to all of these delegates.

As this will be my last CFET conference as Chair, as I am retiring in October, I would like to thank all of the many old and new friends who have contributed to the success of the conferences since CFET 2007. In particular I would like to thank the staff in the Department of Computing who have helped in the organisation of the seven conferences, the many sponsors and the members of the International Advisory Panel who have referred the many valuable papers and papers published in the conference proceedings. All my best wishes for the future.

I would like to welcome everyone to Canterbury Christ Church University and the Centre for Cybercrime Forensics who are playing host to this seventh annual international conference and hope your stay with us is a very enjoyable and informative one.

Denis Edgar-Nevill
Chair, CFET 2014

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

International Advisory Panel

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

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 Associate Professor, Champlain College Vermont, USA

Dr. Rob D'Ovidio Drexel University, USA

Denis Edgar-Nevill Head of Centre for Cybercrime Forensics, Canterbury Christ Church University

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 Embry-Riddle Aeronautical University, USA

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

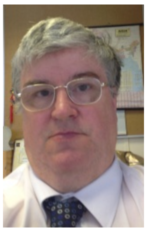
Dr Richard Overill Kings College London

CFET 2014 Conference Programme

Day 1 – 10th July 2014

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

10.30 - 10.45 **Welcome to the University and Conference – Ramsey Lecture Theatre**



Denis Edgar-Nevill, Chair CFET 2014
Head, Centre for Cybercrime Forensics
Canterbury Christ Church University, UK

10.45 - 11.30 **Plenary Presentation (Chair Denis Edgar-Nevill)**

'European Commission Support to Cybercrime Forensics Education & Training'.

Mike Palmer
Policy Officer, Serious Organised Crime Unit
European Commission's Directorate-General for Home Affairs

11.30 – 13.00 **Parallel Presentation Sessions**

Ramsey Rg31 (Chair – Professor Nigel Jones)

11.30 – 12.00 ***"Understanding the Risks and Benefits of Bring Your Own Device (BYOD)"***
Caitlin Toner & George R S Weir
University of Strathclyde

12.00 – 12.30 ***"An Initial Study into BYOD, Cloud and Insider Threats"***
Colin Beeke & Peter Komisarczuk
University of West London

12.30 – 13.00 ***"What Artefacts of Evidentiary Value Can Be Found When Investigating Multi-User Virtual Environments?"***
Madeline Cheah, Lauchlan Wyndham-Birch &Robert Bird
Coventry University

Ramsey Rg36 (Chair –Dr Man Qi)

11.30 – 12.00 ***"Towards Real-Time Profiling of Human Attackers and Bot Detection"***
Avgoustinos Filippoupolitis, George Loukas & Stelios Kapetanakis
University of Greenwich/University of Brighton

12.00 – 12.30 ***“Techniques for the Detection and Monitoring of Malware Behaviour Within Virtual and Cloud Environments”***
Adrian Winckles, Mark Graham & Andrew Moore
Anglia Ruskin University

12.30 – 13.00 ***“A Testbed for Cloud Based Forensic Investigation”***
Zareefa S Mustafa &Philip Nobles
Cranfield University

13.00 - 14.00 **Lunch**

14.00 – 14.45 **Plenary Presentation (Chair Denis Edgar-Nevill)**
“The All Round Cyber Crime and Security Professional – Circular Teaching for the Professional and the Technical - Experiences from the Witness Box”
Adrian Winckles & Andrew Moore
Anglia Ruskin University

14.45- 15.45 **Parallel Presentation Sessions**

Ramsey Rg31 (Chair –Professor Nigel Jones)

14.45 – 15.15 ***“Deepthought: Initial Validation of a Preliminary Analysis Forensic Tool”***
Fergus Toolan, Ray Genoe, Adrian Shaw, Alan Browne & Ulf Bergum
University College Dublin

15.15 – 15.45 ***“An Assessment of Data Leakage in Firefox Under Different Conditions”***
Calum Findlay & Petra Leimich
University of Abertay

Ramsey Rg36 (Chair –Dr Man Qi)

14.45 – 15.15 ***“Undertaking an Activity Led Learning Approach in the Development of an Appropriate Pedagogy in the Field of Digital Forensics”***
Robert Bird & Madeline Cheah
Coventry University

15.15 – 15.45 ***“Continued Development of a Masters Module on “Forensic Computing Using Linux”***
Sarah Morris
Cranfield University

15.45 - 16.00 **Coffee - foyer Ramsey Building**

16.00 – 17.30 **Parallel Presentation Sessions**

Ramsey Rg31 (Chair –Abhaya Induruwa)

16.00 -16.30 ***“Employing Neural Networks for DDoS Detection”|***
Man Qi
Canterbury Christ Church University

16.30 – 17.00 ***“An Analysis of Pre-infection Detection Techniques for Botnets and Other Malware”***
Mark Graham
Anglia Ruskin University

17.00 - 17.30	***"PUA – Potentially Unwanted Advice"*** Righard Zwienenberg & Bruce Burrell ESET

Ramsey Rg36 (Chair –Denis Edgar-Nevill)

16.00 -16.30	***"Education in the Impossible Fight Against Cybercrime"*** Denis Edgar-Nevill Canterbury Christ Church University
16.30 – 17.00	***ECENTRE Development Partner*** Brett Lempereur Liverpool John Moores University
17.00 - 17.30	**ECENTRE Development Partner** Qin Zhou Coventry University

18.30 – 19.00 **Drinks Reception**

19.00- 21.00 **Conference Dinner**

Day 2 – 11th July 2014

09.00 – 10.00 **Parallel Presentation Sessions**

Ramsey Rg31 (Chair – Dr Abhaya Induruwa)

09.00-09.30 ***"Techniques Available for Pattern Matching in Mobile Phone Forensics"***
Ed Day
Canterbury Christ Church University

09.30-10.00 ***"What Do Smart Phones Reveal About Their Owners' Social Identity?"***
Abhaya Induruwa
Canterbury Christ Church University

Ramsey Rg36 (Chair – Dr Man Qi)

09.00-09.30 ***"The Social Media Connection"***
Righard J. Zwienenberg
ESET

09.30-10.00 ***"An Investigation into Privacy and Identity Theft Using Social Media"***
Lily Rose Jenkins & Diane Gan
University of Greenwich

10.00 – 10.30 **Coffee - foyer Ramsey Building**

10.30 – 11.15 **Plenary Presentation – Ramsey Lecture Theatre (Chair Denis Edgar-Nevill)**
***"Programming for Investigators:
From zero to hero in four days"***
Ray Genoe/Fergus Toolan
University College Dublin

11.15- 13.00 **Parallel Presentation Sessions**

Ramsey Rg31 (Chair –Professor Nigel Jones)

11.15-11.45 ***"The Efficacy of the Enron Dataset for Digital Investigation Training and Education"***
Harjinder Singh Lallie, Isabel Oritsematosan Otubu &Roma Manoj Gandhi
University of Warwick

11.45-12.15 ***"A Comparison of Geo-Tagging in Mobile Internet Browsing Applications on iOS and Android"***
S. Comer & P. Leimich
University of Abertay

12.15-12.45 ***"Use of Netflow/IPFix Botnet Detection Tools to Determine Placement for Autonomous VM's"***
Razvan-Ioan Dinita, Andrew Moore, Adrian Winckles & George Wilson
Anglia Ruskin University

12.45-13.15 ***"Analysis of Feodo Malware – a Complimentary Approach"***
Robert Burls & Philip Nobles
Cranfield University

Ramsey Rg36 (Chair –Dr Abhaya Indurwa)

11.15-11.45 ***"The Cyber Security CSI Effect in Bollywood"***
Pulkit Vohra, Roma Gandhi & Harjinder Singh Lallie
University of Warwick

11.45-12.15 ***"Forensic Implications of Portable Operating Systems"***
Charles Frewin & Dr Morris
Cranfield University

12.15-12.45 ***"A Strategic Human Resource Management Model to Develop a High Performance Work System for Cyber Crimes Investigators Within UAE Police Force"***
Jassem I Al Mansoori, Graham Benmore & Margaret Ross
Southampton Solent University

12.45-13.15 ***"Education and Privacy: PIN and Passphrase Selection Strategies"***
David Harley
ESET

13.15 - 14.15 **Lunch**

14.15 – 15.00 **Keynote Presentation – Ramsey Lecture Theatre (Chair Denis Edgar-Nevill)**
"The Legacy of 2Cemtre"

Nigel Jones
TRL Ltd

15.00-15.30 **Plenary Panel Session - Ramsey Lecture Theatre**

15.30—16.00 **Coffee - foyer Ramsey Building**

1600 **Conference Close**

Conference Abstracts Day 1

Invited Keynote Speaker

Michael Palmer
Policy Officer
Serious Organised Crime Unit
European Commission's Directorate-General for Home Affairs

European Commission Support for Cybercrime Forensics Education & Training

Abstract

The European Commission's Directorate-General for Home Affairs has contributed significantly to the fight against cybercrime through policy coordination and funding under its Internal Security Fund. Details of past achievements and future plans in the field will be shared, including a look at the Forensics topics under the Horizon 2020 Programme.

Biography

Mike is a Policy Officer in the Serious Organised Crime Unit of the European Commission's Directorate-General for Home Affairs. As part of the Cybercrime team, his responsibilities include: implementation of the recently adopted Directive on Attacks against Information Systems; following external aspects of EU cybercrime policy, including the EU-US Working Group on Cybercrime; Programme Management and evaluation of EC-funded projects to fight and prevent cybercrime; and support to Cybercrime Centres of Excellence in Training and Education. Mike's previous experience includes 3 years on the 'Technology in Business' stream at the UK Government's Home Office, 3 years as a Project Officer in the 'ICT for Health' unit in the European Commission's DG CNECT, 3 years in the European Parliament and other consultancy roles in Brussels and 4 years in London-based advertising and online marketing positions. He has a degree in Modern Languages from Oxford, a Masters in International Relations from the Université Libre de Bruxelles and an Open University Post-Grad Certificate in Information Technology Professional Practice.

Understanding the Risks and Benefits of Bring Your Own Device (BYOD)

Caitlin Toner & George R S Weir*
Department of Computer & Information Sciences
University of Strathclyde

Abstract

Following an earlier exploratory survey in 2011 (Lazou & Weir, 2011) on smart-phone use, we sought to shed light on recent developments in the use of mobile devices in the workplace. To this end, we established a Web-based questionnaire on BYOD that could be directed at a broad spectrum of end-users, but with a specific interest in users within commercial organisations. In order to direct our search for respondents, small businesses in Scotland were targeted with assistance from the Scottish Business Resilience Centre, through calls for participation on a cybercrime mailing list and through a large LinkedIn group with a special interest in Financial Crime Risk, Fraud and Security.

The aim of our investigation was threefold: (1) to establish a measure of organisational adoption of Bring Your Own Device (BYOD); (2) to estimate the level of associated security risk awareness in end-users; and (3) establish a general purpose on-line survey facility with in-built analytics and data display capability. As well as detailing the content of this BYOD Web survey, the proposed paper will present our initial results and outline our insights on the approach to on-line questionnaire design and associated data analysis.

References

A. Lazou and G. R. S. Weir. Perceived Risk and Sensitive Data on Mobile Devices, in *Cyberforensics: Issue and Perspectives*. Edited by G. R. S. Weir. Glasgow, UK. University of Strathclyde Publishing. 2011. pp. 183-196.

An Initial Study into BYOD, Cloud and Insider Threats

Colin Beeke & Peter Komisarczuk
University of West London

Abstract

Globalisation, economic demands and the ever-increasing need for employee efficiency is pushing technology advancement to allow for anywhere-anytime interaction with enterprise operational services. The ever-growing multicultural mix of societies from a multitude of cultures, beliefs, regulatory/standards and acceptable norms is forcing all forms of organisations within the public and private sectors to rethink their internal security, moving away from their traditional, relatively closed, operational environments. The introduction in recent years of Bring-Your-Own-Device (BYOD) policies, mobile technologies, Wi-Fi and the Cloud have changed the border demarcations of all organisations and the concept of internal versus external threats and attacks. The ever-advancing sophistication of vector threats means that constant flexible threat management systems need to be automated and dynamic in nature, especially as the definition of internal threat is also evolving across all commercial sectors. The complexity of the mix of employees' ever-advancing array of devices and features, together with the Cloud's offer of enterprise resource storage, daily operation and customer services leads to a socio-technical approach to meet the aim of providing a holistic security approach for enterprises to reduce the potential risks imposed by BYOD and Cloud utilisation.

Present research uses limited data, predominately from cases that have involved legal intervention or have become known to the public. Given that prevention is better than cure, this research aims to be proactive in its approach, to determine the true depths of the problem through online surveys which will create a longitudinal study and an online forum to engage in a less structured manner. Additionally new EU regulations require all member countries to make security breach reports available and thus this rich new data source can be used to determine the range of threats and solutions more effectively as this data set becomes available. However it must be recognised that each enterprise is unique, and must create a unique solution based upon its market sector, best practice and awareness of potential issues, therefore a framework for effective analysis will be required.

To begin this research an initial survey was conducted among a target population of 26 part-time students at the University of West London, who work within the IT sector, in order to gauge willingness to divulge their knowledge of insider activities and threats. Of the respondents practically all admitted to using employer technology for personal use, 11 indicated they were aware of their employers having to take action due to security issues, 14 could provide details of know security threats within their organisation and 2 requested details of this research to take back to their employers. Present student projects being conducted are showing signs of a wide range of security issues against

What Artefacts of Evidentiary Value Can be Found when Investigating Multi-user Virtual Environments?

Madeline Cheah, Lauchlan Wyndham-Birch and Robert Bird
Coventry University

Abstract

Muti-user virtual environments (MUVEs) such as Minecraft are digital spaces where an individual is immersed in a virtual environment for a multitude of purposes. Such multi-faceted tools can also be used to enhance teacher training and education, as well as serve a purpose as an education tool for children, enabling them to develop skills such as social awareness, creative thinking, spacial awareness and geometry (Rock, 2013).

In such environments, user-to-user interaction is essential, but this brings with it some negative aspects. There is an ethical dimension to the activities that users engage in and as in the “Real World,” behaviours’ exhibited and situations occur that “mirror” reality. Online servers suffer from relatively benign acts such as “griefing” (logging in to destroy other users' creations) or abuse of services. However, interactivity can also bring with it the risk of grooming, conspiracy to commit crimes, security exploits, cyber-bullying or other criminal activity (Shute, 2013). Although these are also prevalent offline, processes to investigate such behaviour or activity are well established. It is technically possible to monitor MUVEs (Vijayan, 2013), however, finding articles after the fact is down to individual implementations with regards to the level of detail, where the log files might be found and the criteria for activity or articles of interest. The determination of an overall structure of how and where digital artefacts of interest can be located, when investigating these kinds of criminal activity, have yet to be elucidated.

This study explores how and where artefacts of interest can be found with regards to popular virtual environments within its necessary associated configuration files and server logs. This is also in accordance with digital forensics principles should the need for a criminal investigation ever arise. Acquisition and analysis of evidence involved the use of a variety of specialist tools, such as NBT Explorer (a tool for Minecraft data files) (Jaquardro, 2011) and, because of the digital forensics context of this study, follows the generally accepted ACPO Good Practice Guide for Digital Evidence (ACPO, 2012).

Experiments and exploration of the data files and network activity show a surfeit of artefacts, with the vast majority being of evidentiary value. This includes timestamp-ed activities performed in-game, events such as logins and logouts, repeat login attempts from the same user, chat logs and user settings with regards to the game. Items are stored both offline and on the server-side. However, these artefacts are scattered and require a lot of human resource in order to find, and additionally, the volatility of these artefacts have not yet been verified or validated. The authors of this paper seek to use this as a model to continue investigating the most prevalent artefacts (and just as importantly locations of prevalent artefacts) in online MUVEs.

Although this paper uses Minecraft as an example, as the use of global games increases, with ever younger audiences, these methods and artefacts could prove invaluable during the course of an investigation. This study also demonstrates that while it would be impractical and possibly unfeasible for all developers to keep in mind digital forensics whilst developing these programs, there is still a need for application developers to consider a general purpose logging methodology. In any case, the potential misuse of the likes of Minecraft, or for data to be obfuscated for nefarious purposes, render it a useful area of investigation.

Techniques for the Detection and Monitoring of Malware Behaviour within Virtual and Cloud Environments

Adrian Winkles, Mark Graham and Andrew Moore
Anglia Ruskin University

Abstract

For both enterprises and service provider's, the exponential growth of cloud and virtual infrastructures brings vast performance and financial benefits but this growth has undoubtedly introduced unforeseen problems in terms of new opportunities for malware and cybercrime to flourish. Botnets could effectively be created entirely within the cloud with virtual resources for myriad of purposes but the potential for DDoS on demand would appear obvious and in fact this could become DDoS as a Service.

This study has sought to determine whether distributed packet capture utilising mirroring technology or some form of sampling mechanism provide better performance for detecting cybercrime style activities within virtual environments and make recommendations for a distributed monitoring technique in cloud and virtualised environments which can provide end to end monitoring capabilities while minimising the performance impact on popular adoptions of cloud or virtual infrastructures.

Investigations have concentrated on distributed monitoring techniques utilising virtual network switches or equivalent technologies, looking for a proof of concept demonstrator where sample C&C and P2P botnet activities can be detected by a distributed monitoring system utilising flow measurement technologies such as Netflow, Sflow or IPFIX.

By considering how the monitoring function can be inserted into two or more vendor based virtual or cloud architecture environments and evaluation of the effectiveness of the various placements of the monitoring function, existing open source based tools can be leveraged to develop a proof of concept

A Testbed for Cloud Based Forensic Investigation

Zareefa S Mustafa1, Philip Nobles2
Centre for Forensic Computing and Security
Cranfield University

Abstract

Cloud computing is a new technology which gives businesses and individuals on demand, pay as you go access to a shared pool of computing resources via the internet to carry out their transactions using a wide range of devices. It saves cost, space and it changes the traditional look of business environment, but this technology is not without limitations and risks.

Many researchers have reviewed the security and digital forensic investigation challenges of the cloud. In cloud computing, data is stored in remote locations and users have limited control over their data and the underlying physical infrastructure. In terms of digital forensics, this new cloud security perimeter stemming from the trend with which data is now accessed via the internet, housed and consumed on multiple systems and devices in multiple jurisdictions, will pose some serious challenges (legally and technically). This has the potential to complicate an investigation by making it difficult to determine: where the data is, who owns the data, and how to acquire the data.

This paper identifies the requirement s for setting up a testbed for digital forensic cloud computing research. The testbed created during this research used Xen Cloud Platform, XCP, which is an open source server virtualization and cloud computing platform and Citrix XenCentre which is a windows graphical user interface management tool for managing XCP hosts. A basic set up was used with two machines. On the first system XCP 1.6 was installed and local storage configured. The second system had the XenCenter installed on it to provide a graphical management interface for the XCP host.

This paper discusses cloud forensics and focuses on how to set up a private cloud within a lab environment to carry out a forensic investigation. It identifies potential artefacts that can be extracted from a computer that has been used to connect the cloud and the artefacts that can be recovered from the Cloud Service Provider, CSP. It explains different methods of data acquisition and the tools that can be used to analyse the data.

Keywords: cloud computing, digital forensics, cloud forensics

The All Round Cyber Crime and Security Professional –Circular Teaching for the Professional and the Technical - Experiences from the Witness Box

Adrian Winkles and Andrew Moore
Anglia Ruskin University

Abstract

In these challenging times of daily and ever increasing data and security breaches, our cyber security professionals need the hard technical skills to meet the rapidly increasing complexity of cyber conflict but repeatedly this must be combined with the softer but no less essential skills of knowing how to recover data in a forensically sound manner, be able to summarise the data in laymen's terms and be able to stand up to scrutiny of their findings within various legal context's.

On our security and forensic courses we have experimented with a successful combination of these hard and soft skills where we provide Forensic and IT Security students with a relevant Crime Scene Scenario – Live Memory Capture and Digital Evidence Seizure. This involved both promoting the discussion on contamination of evidence – reference to ACPO/NIST Digital Evidence Guidelines as well as the conventional evidence gathering at the custom built crime scene.

Externally to the crime scene students are prepared for forensic handling and analyzing the evidence with specific emphasis on report writing and summarisation skills with the ultimate goal of writing an Independent Witness Evidence Report based on the forensic analysis of the evidence found.

The final demanding challenge for the student is the Court appearance as an independent witness and being able to support the independent witness report under cross examination by both prosecution and defence. Using a combination of retired judges, retired magistrates, ex police officers and current law students, an authentic court room experience can be achieved.

Students reinforced the success of the approach with detailed supporting reflection on what the independent witness experience insight brings to the well rounded cyber professional.

Deepthought: Initial Validation of a Preliminary Analysis Forensic Tool

Fergus Toolan, Ray Genoe, Adrian Shaw, Alan Browne, Ulf Bergum
University College Dublin

Abstract

Digital forensics units are often characterised by the backlogs of devices waiting to be analysed. This is mainly due to the limited number of commercial forensic tools available to the unit and compounded by the fact that up to 70%-80% of devices may not contain any evidential material at all. Digital forensic units are not only limited by software resources, but also by hardware. Running a full forensic analysis on a device is a time-consuming task, that will utilise a forensic workstation for a significant amount of time (often days). During this time, only one device can be analysed. This paper presents a preliminary analysis tool known as Deepthought, which can be used to alleviate this problem.

Deepthought is an open-source solution that automates a forensic examination on a device, in order to determine the presence of evidential material. Since it is based on a live-Linux distribution, it only uses the resources of the device being examined to conduct a preliminary analysis. This means that a forensic workstation is not required for this stage of the forensic process, thereby freeing up the software and hardware resources of a digital forensics unit. If there is no evidential material discovered by Deepthought, the device can be excluded from an investigation. However, as it currently stands, when evidential material is found on a device it must be analysed by trusted commercial forensic tools, such as EnCase or FTK. This is due to the fact that the results of Deepthought are not yet accepted by the court system. While Deepthought has already been used to reduce the large backlogs of forensic units, this paper will propose a method for validating Deepthought so that the re-analysis by commercial tools can be eliminated.

This paper will present the results from the initial test phase of Deepthought. The first goal of this test phase is to prove that the tool is forensically sound and does not alter any of the evidential data being analysed. The second goal is to prove that the tool can recover as many picture files as its commercial counterparts. An extensive data set of picture files was created in the live file system, both as individual files, and as pictures embedded in other documents. The picture task was chosen for the first stage of testing, due to the prevalence of child exploitation cases in the digital forensics sphere.

The initial results show that not only are the processes of Deepthought forensically sound but that image retrieval is comparable to trusted commercial tools.

An Assessment of Data Leakage in Firefox Under Different Conditions

Calum Findlay and Petra Leimich
University of Abertay

Abstract

With millions of people now using the internet for everyday tasks such as online shopping, banking and communication, online security and reducing personal footprint is a crucial area of research. Therefore, the aim of this project is to evaluate the levels of privacy provided by the Firefox browser by comparing data leakage in normal, private and portable browsing modes.

The main areas where data leakage may occur are the focus of this investigation: Firefox's SQLite database and Sessionstore and the host computer's RAM/virtual memory. Firefox introduced private browsing in an attempt to provide users with more privacy online. This is claimed to work in the same way as normal browsing but without storing user information. Both normal and private browsing modes are used and compared to assess the least data leakage.

The approach to this project was experimental and was carried out with in the following three stages:

> 1.) Browsing Stage
> Browsing sessions were carried out with a pre-planned set of activities. Similar web browsing sessions and email interaction sessions were carried out in both normal and private browsing modes of Firefox. Each test was carried out within a fresh virtual machine to ensure reliability as no previous history would be recovered. In order to avoid potential confounding effects that could be introduced by Mozilla's rapid release of Firefox versions every few weeks, this work has been standardised on version 26;
>
> 2.) Acquisition stage
> To capture the data, a snapshot of the current RAM was taken within VMware while the browser was still running, followed by a second snapshot taken after the browser had been closed. An image of the virtual machine was then taken using FTK Imager. These capture methods were repeated for each Virtual machine test;
>
> 3.) Analysis Stage
> The hard drive image created was loaded within Autopsy 3 and a keyword search, specific to the browsing session, was carried out. Secondly, all the Firefox related browsing files were investigated using SQLite Spy for the database and a JSON viewer for the session store. Lastly, using HxD hex editor, both snapshots of RAM and virtual memory were investigated;

The results show that a lot of data leakage may occur within Firefox. Firstly in normal browsing mode, all of the browsing information is stored within the SQLite databases in the Mozilla profile folder. Information such as Cookies, entered form history, visited hosts and downloads etc are all stored within these SQLite databases. While passwords

were not stored as plain text, other confidential information such as credit card numbers could be recovered from the Form history under certain conditions. Moreover Firefox also stores session information in a JSON session file (sessionstore.js), this contains a full detail of the tabs and browsing information from these tabs.

When deleted, this information remains recoverable forensically as shown for example by Bagley et al (2012). By comparison private browsing reduces data leakage by not writing any information to the Firefox-related locations on hard disk. As data was not written to disk, no deletion would be necessary and no data would be recoverable from unallocated space.

However, two aspects of data leakage occurred equally in private and normal browser modes. Firstly, all of the browsing history was stored in the live RAM and was accessible while the browser was open; while significantly less, some artefacts could still be recovered from live RAM after the browser was closed. Secondly, in low RAM situations, the operating system caches out RAM to pagefile.sys on disk, where it can remain accessible semi-permanently as shown by Eleuterio (2011). This data leakage to virtual memory was observed in both Windows and Linux operating systems, and private browsing mode did not prevent the caching out of Firefox artefacts. Portable Firefox, run from a separate pen drive, was also analysed.

Initial results have shown that while all Firefox related files were isolated to the pen drive, the data leakage to RAM and pagefile.sys described above also occurred, confirming findings by Ohana et al (2013). As this project is focused on desktop applications, future work will be to analyse the data leakage on mobile devices.

Undertaking an Activity Led Learning Approach in the Development of an Appropriate Pedagogy in the Field of Digital Forensics

Robert Bird and Madeline Cheah
Coventry University

Abstract

Digital Forensics as a subject of academic study has been evolving over its relatively short life span. As such, the pedagogy associated with it is an area which is relatively ill-defined although there are forums which seek to promote good practise and share teaching experiences (HEA, 2013). This paper seeks to catalogue the methodology used at undergraduate and postgraduate level with respect to the teaching of digital forensics and present it as best practice with regards to activity-led learning in this field. As such the mode of delivery, use of laboratory time, assessment criteria and statistical validation of the approach is detailed.

One of the elements, an alien concept to many students, is that of “investigation”. There is a temptation for curricula to focus upon software tools and competence in using them which, whilst a key element, needs to be underpinned by a thorough comprehension of what “investigation” is and its limitations, as well as how the guiding principles of the ACPO Good Practice Guide for Digital Evidence (2012) apply. Whilst the ACPO Principles lack the status of bona-fide legislation, it is conceivable that substantial non-compliance would equate to inadmissibility as evidence. The legislative context pertaining to the digital environment might be viewed as a law enforcement environment, however, it is increasingly clear that the significance of digital evidence in a corporate context is growing. To that end, activity that focusses upon the discovery of potential digital artefacts, rather than simple searching of digital media for “evidence” is a key pre-cursor to the latter activity. The testing of competencies and comprehension of robust digital recovery is an initial focus for qualitative coursework which examines the application of learned procedures. Further substantive assessment in the form of a “Phase Test” enables the testing of deeper learning as well as competence in using software tools. As an enhanced variant of professional certifications relevant to the digital forensics profession, this reinforces an element of constructive alignment with industry. The validation of its perceived value and fairness is represented in student feedback concerning its use.

Activity-led learning is a pedagogy in which the motivation for learning is provided by stimulating activity that engages students and creates challenge, relevance, integration, professional awareness and variety. Fundamental to this is the use of “industry standards” in digital forensics in order that the “real world” relevance of the teaching and learning is consistently emphasised. This is a learning philosophy designed to produce graduates who have confidence in their ability, capability to achieve and capacity to reflect and innovate (Wilson-Medhurst et. al, 2008) which will positively impact subject learning and, ultimately, employability.

Continued Development of a Masters Module on "Forensic Computing Using Linux"

Dr Sarah Morris
Centre for Forensic Computing,
Cranfield University

Abstract

Since 1998 the Centre for Forensic Computing at Cranfield University has offered short courses aimed at providing education to practitioners. In 2003 the Centre adapted the short courses to form a part time MSc program; in 2011 a full time version of the MSc was introduced. The Forensic Computing Using Linux Course was added to the program in 2007 and was developed to allow students to take the course as both a module on an MSc program, or as a short course. Since the introduction of this module both Forensic Computing Education and Linux Distributions have evolved; this has led to substantial changes to the content and delivery of the course.

Currently the aim of the module is to "develop a practical working knowledge and understanding of Linux, and open-source tools, as a platform for performing computer forensic examinations". In order to meet this aim the syllabus currently covers a wide range of general Linux topics alongside sessions on forensic software, and the development of a forensic workflow. The course is taught over a single residential week with each lecture having a practical element; this provides the students with an opportunity to explore each concept using a structured practical as it is introduced to them. On the last day of the week the students are examined on the material. Accredited students also complete a piece of coursework.

For the next iteration of the course this paper proposes the development of material on portable Linux based devices and their role in the forensic computing devices. The paper also suggests the requirements for improving existing course content. Following the results of this research it is also proposed to change the assessment of the module through a practical exam and a scenario based coursework. The paper also highlights methods which could be used to strengthen the existing pre-work given to students a month before the residential module runs. In a recent restructuring of departments the Centre for Forensic Computing has joined the existing Cranfield Forensic Institute, leading to access to a wider range of forensic resources for teaching and research; this paper discusses the impact of this restructuring on the development of this module.

This paper examines the current state of the Forensic Computing Using Linux Module and looks at the system used for reflection and development of the module. The paper then examines alternative methods which could be used to assist the continual development of the module. This paper also includes a discussion on concepts which should be included when teaching Linux for Forensic Computing; this leads to a set of proposed course changes for the next iteration of the module. This paper contributes to a growing discussion with both the academic and law enforcement communities.

Employing Neural Networks for DDoS Detection

Man Qi
Department of Computing
Canterbury Christ Church University

Abstract

Neural Network based on statistical features is widely used to classify DDoS attack patterns [1]. The Neural Network approaches have advantages of self-learning [2] that enable them to detect new DDoS attack patterns besides detecting known DDoS attack signatures. They have disadvantages too. One of them is neural computational overhead [3]. This paper is to overview the Neural Network DDoS detection methods. An approach [4] uses neural network to detect DDoS attack towards DNS servers. In this method several attack characteristics are extracted from DNS Server queries and these attributes fed into Neural Network Classifier. The simulation results show that Two-Layer Neural Network DDoS detection method which consists of Hidden and Output layer has low false alarm. The overhead of the method has direct correlation with the number of epochs of training. By increasing the number of epochs the computational overhead can be exponential to the number of epochs. Another method [5] proposes a detection method based on Neural Network. In this method neural network is used as an analyser and composed of the offline training part and the online analyser. Training of neural network will be done offline first. When an attack occurs online analyser sends filtering message. In [2] a method is proposed for DDoS detection based on Host anomaly detection. In this method some DDoS attacks are trained to Learning Vector Quantization (LVQ) neural network to enable them to detect new attacks. The most important result of this method is the comparison between Back Propagation (BP) Neural Network based method and LVQ Neural Network based approach in detecting DDoS attacks. As shown in the work the accuracy of LVQ Neural Network is about 99.732% while in BP Neural Network based methods the best result was 89.9%. This paper will show the major implementations of Neural Network for DDoS detection.

References

[1] Jun Li, Constantine Manikopoulos, Early Statistical Anomaly Intrusion Detection of DOS Attacks Using MIB Traffic Parameters, IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, June 2003

[2] Jin Li, Yong Liu, DDoS Attack Detection Based On Neural Network, IEEE 2nd International Symposium on Aware Computing (ISAC), 2010

[3] P. Arun Raj Kumar , S. Selvakumar, Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems, Elsevier Journal of Computer Communications, No 36, 2013

[4] Jun Wu, Xin Wang, Detecting DDoS Attack towards DNS Server Using a Neural Network Classifier, Springer Journal of 20th Conference of European Neural Network Society, Page 118, 2010

[5] Dongqi Wang, Zhu yufu, A Multi-core Based DDoS Detection Method, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010

An Analysis of Pre-Infection Detection Techniques for Botnets and Other Malware

Mark Graham and Adrian Winckles
Anglia Ruskin University

Abstract

Traditional techniques for detecting malware, such as viruses, worms and rootkits, rely on identifying virus-specific signature definitions within network traffic, applications or memory. Because a sample of malware is required to define an attack signature, signature detection has drawbacks when accounting for morphism, has limited use in Zero-Day protection and is a post-infection technique requiring malware to be present on a network, or device, in order to be detected.

A malicious Bot is a malware variant that interconnects with other Bots to form a Botnet. Amongst their multiple malicious uses, Botnets are ideally suited for launching mass Distributed Denial of Services (DDoS) attacks against the ever increasing number of networked devices that are starting to form the Internet of Things, and ultimately Smart Cities.

Regardless of topology; centralised with Command & Control servers (C&C), or distributed peer-to-peer (P2P), Bots must communicate with the other Bots in the Botnet, as well as their overall commanding Botmaster. This communication traffic can be used to detect malware activity in the cloud, well before it has been able to evade network perimeter defences and trace a route back to source to takedown the threat.

This paper reviews the various methods available today for pre-infection detection of malware, concluding that Cloud centric traffic based detection techniques can be used to complement traditional signature based anti-malware, and overcome some of its drawbacks. This paper goes on to highlight the lack of techniques for detecting malicious Bot activity within Virtual Environments, which now form the backbone of data centre infrastructure, and provide a new, as of yet untapped, attack vector for future malware.

PUA – Potentially Unwanted Advice

Righard Zwienenberg and Bruce Burrell
ESET

Abstract

For a long time now, security experts have advised users to use ad-blockers, pop-up blockers, and other browser plugins/add-ons such as “NoScript” to create a safer environment while browsing the internet.

Recently we have observed a trend among websites to alert visitors that in using these added layers of protection (these blockers and/or browser plugins/add-ons) they are running a risk. Given that some add-ons and plugins are unequivocally malicious, this may be correct in the strictest sense, but the motivation of these websites often seems financial or even malicious rather than altruistic, and the suggestion is ill-advised.

Another problem is the use of the installation framework that software download sites are likely to use. These sites wrap the original software into an installer package that, on execution, advises the user to also install other – often sponsored – software or, even worse, install these without the user’s consent. This can result in unwanted and sometimes amusing situations, but can be very confusing for the end user.

Our paper will examine the relationship between the blockers and plugin/add-ons, the advice commonly given and the possible implications of following that advice from a user, website and security vendor’s point of view, and also discusses the confusing situations that can arise when using installers for software obtained from websites other than the vendor’s own site.

Points to cover

1. Pros and cons of using blockers and plugins/add-ons
2. Overview of all kinds of blockers and plugins/add-ons
3. The problems with the advice often given
4. Data Leakage consequences of following the advice
5. The problems around installing applications from download sites

Education in the Impossible Fight Against Cybercrime

Denis Edgar-Nevill
Centre for Cybercrime Forensics
Canterbury Christ Church University

Abstract

Some sources now put Cybercrime as bigger (in terms of money) than the distribution and sale of all forms of illegal drugs trafficking worldwide. It is certainly responsible for the greatest number of attempted crimes of any type and the problem is growing rapidly. Kaspersky Labs reported that in 2012-2013, phishers launched attacks affecting an average of 102,100 people worldwide each day – twice as many as in 2011-2012. The 2013 Norton Cybercrime Report around one million adults become Cybercrime victims everyday with an average cost to each of $298.

It's foolish to believe there is any single magic bullet to combat Cybercrime. Governments around the World have committed massive sums of money to fighting threats to national cyber-infrastructure but the key question is where it's best to spend your money? The analogy is that you are standing under a tidal wave with an umbrella (a very good umbrella) but don't expect it to keep you dry. If you don't study Cybercrime and Computer Forensics how can you avoid every day being a Zero-Day Problem? (i.e. when an attack occurs, you have to waste considerable time bringing yourself up-to-speed with the current state of the technology before you can plan and implement how to deal with the attack).

The European Union recognised the increasing threat to trade and the personal well-being of EU citizens with the EU *Convention on Cybercrime* in Budapest on 23rd November 2001. This was one of the first formal statements clarifying the nature of the Cybercrime threat. Since 2001 the EU has funded a number of development, research and training initiatives most recently under the ISEC Programme. This has financed the creation of national Centres of Excellence starting with the 2Centre Project in Ireland and France and, in the last 4 years with centres in a range of other member states. My own involvement is based on our work leading the ECENTRE (England's Cybercrime Centre of Excellence for Training Research and Education) project (€1 million over 20 months involving 10 UK Universities 4 companies and the College of Policing in the UK). This project began in December 2012 and concludes in August 2014. It includes major training and skills updating for law enforcement in the UK/EU and brings together the three important areas of law enforcement, commerce and the university sector. Each of these areas brings valuable expertise, experience and opportunities to help education and defend organisations and individuals from the developing threat of Cybercrime. The cooperation of such national centres is important and the creation of EC3 (the European Cybercrime Centre) within Europol on January 2013 provides a major exchange for information and joint initiatives. But by comparison with the problem these initiatives are small.

Techniques Available for Pattern Matching in Mobile Phone Forensics

Ed Day
Canterbury Christ Church University

Abstract

Mobile phone forensic extraction tools such as such Paraben's device seizure create reports containing information about a phone's contents. It can be useful for law enforcement to use these data to explore associations between different phones to discover relationships in criminal networks. This matching of phones can be done at the phone level (either physical or logical representation), the file level, the part file level or the file content level. Phones and their data can be exactly or approximately matched. Exact matching is a relatively trivial problem and existing software such as Threads can provide a useful summary of how a phone matches to others. However there may be further less obvious associations between phone data, which can be investigated using approximate matching (AM) techniques.

Semantic AM matching involves the interpretation of properties of digital artefacts, ignoring the lower level details of digital data. Robust hashing (RH) and Natural Language Processing (NLP) are examples of semantic AM.

RH can be used in image, audio and video identification (Yannikos, 2013). There are a number of RH methods in the literature for images, for example hashing an image's colour attributes (Sarohi & Khan, 2013) or perceptual hashing methods which calculate averages based on the low frequencies of an image (Krawetz, 2011). Haitsma et al (2001:3)'s RH for audio scheme sampled audio files in 3 second segments and calculated how these many of these were different between audio samples. Polastro & Eleuterio (2010, 2012) developed a forensic tool, NuDetective Forensic that uses a RH scheme on samples of video in order to automatically detect child pornography.

NLP is the process of extracting the meaning (or semantics) of a text (Kao & Poteet, 2007). Usually text is normalised, classified and entity, event and relations are extracted from it (e.g. an entity might be "member of gang"). There are a number of different approaches to developing NLP applications for forensic matching. For example Ishihara (2011) used NLP techniques for investigative purposes by using n-gram analysis to determine the likelihood of authorship classification.

This work aims to investigate how do we interpret matching similarities, and how do we decide if we have a match at the phone level. Also, since these processes are computationally expensive, can we scale phone matching processes using the Apache Hadoop framework?

References

Haitsma, J., Kalker, T., & Oostveen, J. (2001). Robust audio hashing for content identification. In International Workshop on Content-Based Multimedia Indexing (Vol. 4, pp. 117-124).

What Do Smart Phones Reveal About Their Owners' Social Identity?

Abhaya Induruwa
Department of Computing
Canterbury Christ Church University

Abstract

The emergence of smart phones such as iPhone, Android, Blackberry, etc., has changed the way mobile phone users interact with each other. Over the years people have progressively moved to always connected high speed Internet access (3G/4G technology) and to social networking applications such as Facebook, Twitter, vKontakte, Fring, HeyTell, ICQ, WhatsApp, etc. With the modern smart phones resorting to SQLite type databases to store all user information the process of deletion in a smart phone has a new meaning.

While smart phones are becoming smarter by the day, mobile phone forensic tools are also becoming capable of extracting more data about mobile phone users and their behaviour. The modern tools are capable of extracting and analysing patterns of behaviour in addition to reporting the standard outputs such as phonebook, call log, SMS/MMS messaging, calendar, tasks and appointments, Wireless (SSID, location) activity, Internet activity (web surfing, downloads), etc. The work of Al Mutawa et al (2012) is limited to extracting social networking activity data from MySpace, Twitter and Facebook on three popularly used smart phones but only one phone at a time. Mulazzani et al (no date) describe how social interaction graphs, event tracking and time lines can be visualised by downloading user's data from Facebook accounts. Although the former study used EnCase to examine the backups the forensic value of the latter is questionable. This case study illustrates how the features available in Oxygen Forensic Suite such as aggregated contacts, dictionary analysis, social networking data showing complex relationships between members/groups (social graphs, gang crowding), almost automatic password cracking and recovery, and geo location data (GPS runs), can be immensely useful to mobile forensic investigators. A comparative study of the latest versions of three industry standard mobile phone forensic examination tools (Oxygen Forensic Suite, XRY, RTL Aceso) in terms of their ability to extract, analyse and report social networking information will be carried out and their capabilities will be presented.

References

Al Mutawa, N., Baggili, I., and Marrington, A. (2012) "*Forensic analysis of social networking applications on mobile devices*", Digital Investigation (9), pp 24-33

Mulazzani, M., Huber, M., and Weippl, E., (no date) "*Social Network Forensics: Tapping the Data Pool of Social Networks*", Available at: https://www.sba-research.org/wp-content/uploads/publications/socialForensics_preprint.pdf, Accessed on 16 March 2014

The Social Media Connection

Righard J. Zwienenberg
ESET

Abstract

The latest threats have one thing in common: in one way or another they are all using Social Media. Social Media is of course nice, fun, a way to stay in contact with your friends and a way to "share" yourself. But it also carries unexpected dangers. These include not only accidental but unwanted exposure (specifically, pictures), but also to malicious URLs and cybercriminal activities like click-jacking. With a little social engineering to get you to click the links and… take you for a bumper car ride down the cybercrime lane showing that once something is on the internet, one way or the other, it is always available, even if you think it has been removed.

The presentation explores various aspects of Social Media, the different dangers from both the social and cybercriminal point of view, and the potentially irreversible and damaging consequences of unexpected exposure. Each example will be illustrated by real-life stories, some with less than desirable consequences, to say the least.

Although not all problems can be solved by security solutions, examples and suggestions are given to better protect the end-user, both at home as well as at the corporate end-point. Those who think that the corporate end-points are not at risk are ill advised.

Key points:

1. Trust and mistrust: the provider
2. Trust and mistrust: friends, relatives, lovers, sexting and sextortion
3. Social media and the workplace
4. Mapping cyberspace

An Investigation into Privacy and Identity Theft Using Social Media

Lily Rose Jenkins and Diane Gan
University of Greenwich

Abstract

Most teenagers today have at least one “profile” on a number of social networking sites, such as Facebook or Twitter, where they reveal a lot of personal information about themselves that anyone can see and use. These types of social network sites are used by young people without them realising the dangers that they are exposing themselves to. Twitter currently has 200 million active users who send over 400 million tweets per day, most of which are publicly available. Many Twitter users do not realise that features such as their location and their identity are turned on by default. Often Twitter users have the same picture of themselves and the same handle (username) on all their social media sites, which makes it even easier to identify them and follow them through cyber space to harvest more personal information about them from their Facebook pages and other sites. A series of experiments were run using test subjects who had agreed to allow their tweets to be harvested in order to determine how much information could be gathered about them, using social media. A number of different software tools were used to extract tweets, geo-locations and images to build a profile of each subject. Using geo-location tagging, tracking, an individual’s tweets and their profiles, a lot of information about each of the volunteers was gathered and the results are presented.

All the tools used in the experiments were freely available. One tool which is particularly efficient at extracting information on individuals was Creepy. This was advertised as a “geolocation aggregator” which not only harvested information from social media networking sites, but from image hosting services as well. The result of using this tool was a trail of tweets and locations giving latitude and longitude and also dates and times of the tweets. These appeared as a cluster of location pins which were mapped onto Google earth. If the subject was a prolific tweeter it was possible to identify their home location, their exact route to work and their workplace. It was also possible to use other social media to extract further information about that individual and even to be able to obtain a picture of their front door. The danger identified by this work was that this information could be used for criminal activities such as stalking or identity theft.

This work has investigated the privacy issues that are present on social networking sites and the results are presented.

Programming for Investigators: From Zero to Hero in Four Days

Ray Genoe, Fergus Toolan
University College Dublin

Abstract

Traditionally courses for Digital Forensic examiners focused on the use of tools for examining suspect devices. In doing this LE personnel were taught some basic theory, such as file systems, networking, etc. However little, if any time was spent teaching LE personnel the more traditional aspects of computer science such as programming. Investigators require programming skills for numerous reasons such as: automating manual repetitive tasks; analysing newly encountered artefacts; or for extending the capabilities of existing forensic software. However, investigators are often intimidated at the thoughts of writing computer programs, feeling that their training / experience does not allow them to develop effective programming solutions.

This paper presents an intensive programming course aimed specifically at investigators which was developed by the authors as part of the 2CENTRE project. The course is aimed at investigators who have limited past programming experience. The course is developed with investigators in mind throughout. The examples used in the course are scripts that the investigator may have cause to use in the course of investigations. Some of these topics include log file analysis, web site monitoring, and handling Unicode character encodings. All of these topics were chosen through informal consultation with investigators in the field, indeed, in many cases the authors were asked by investigators to solve these problems for ongoing investigations.

This paper describes the curriculum developed for the course and also the teaching methodologies employed. Rather than a dry theoretical course, this course revolves around student participation. From the moment that student commence the course they begin to write simple Python scripts. This gradually leads up to the development of forensic applications within four days. The course begins with basic programming constructs such as input / output, assignment, selection, iteration and functions. It then introduces regular expressions and Unicode character handling. The course culminates in students developing forensic applications. At the time of writing this paper the author's have run the course three times as an intensive Continuing Professional Development (CPD) course. From each of these deliveries student feedback was gathered each day of the course from every student. In the main this feedback was extremely positive from the majority of students. Some changes were incorporated into the material based on the feedback received from students. Also students were asked to provide feedback a few months after completing the course. From this we discovered that a significant portion of the students were still using the skills taught in the course, and have also been generating widespread interest in the course through demonstrations of these skills to their respective colleagues.

The Efficacy of the Enron Dataset for Digital Investigation Training and Education

Harjinder Singh Lallie, Isabel Oritsematosan Otubu, Roma Manoj Gandhi
University of Warwick

Abstract

The lack of suitable case studies for use in Digital Investigation related courses in academia has previously been well documented (Lallie 2010). A number of solutions to this probem focus on the automated development of file systems (Jones 2010; Tohill 2013) and in a variety of cases, sample digital forensic images have been published which can be investigated by students. Examples of these include a number provided by NIST through the CFReDS (Computer Forensic Reference Data Sets) Project (CFReDS (NIST) 2007), a set of digital forensic images published by Brian Carrier (Carrier 2010), a series of images published by Lance Mueller (Mueller 2010), a sample by the International Society of Forensic Computer Examiners (ISFCE) (The International Society of Forensic Computer Examiners (ISFCE) 2014) and Digital Corpora (Digital-Corpora 2011)

The problem with most of these case studies is that the answers are easily available and there is a high potential of plagiarism. Furthermore, the case studies are all based on fictional data and there is an argument that these may not adequately prepare students for real experience in industry.

The Enron Dataset contains Email messages captured from November 1998 to June 2002 representing day-to-day business and social activities of 158 of Enron Employees. The original dataset was made public by FERC (Federal Energy Review Commission) and numerous versions have been released since. The dataset was made public in an attempt to demonstrate openness and transparency in the investigation that took place into the massive fraud conducted by the CEOs of Enron in collaboration with colleagues in Arthur Anderson. Versions of this dataset contain between ½ million to 1.3 million email messages of more than 150 members of staff.

In this paper we explore the efficacy of the Enron dataset as a case study for digital investigation and explore how this can be used in academia for teaching students. We select four accounting fraud scenarios and demonstrate the range of tasks that students can be asked to investigate.

References

Carrier, Brian (2014), 'Digital Forensics Tool Testing Images', <http://dftt.sourceforge.net/>, accessed 20th March, 2014.

CFReDS (NIST) (2011), 'Hacking Case', <www.cfreds.nist.gov/Hacking_Case.html>, accessed 6-7-11.

Digital-Corpora (2011), 'Digital Corpora', <http://digitalcorpora.org/>, accessed 8th July, 2011.

Jones, M. (2010), 'A Digital Forensics Case Generator', *4th International Conference on Cybercrime Forensics Education and Training* (Canterbury Christchurch University).

Lallie, Harjinder Singh (2010), 'Developing Usable hard disk images for Forensic training, education and research', *4th International Conference on Cybercrime Forensics Education and Training* (Canterbury Christchurch University).

Mueller, L 'Forensic Practical Exercise', <http://www.lancemueller.com/blog/evidence/Forensic_Practical_3.E01 >, accessed 8th July, 2011.

The International Society of Forensic Computer Examiners (ISFCE) (2014), 'Sample Practical Exercise Problem', <http://www.isfce.com/sample-pe.htm>, accessed 20th March, 2014.

Tohill, Sean (2013), 'Tool Based Generation of Disk Images for Teaching', *8th Teaching Computer Forensics Workshop* (University of Sunderland, UK: HEA).

A Comparison of Geo-Tagging in Mobile Internet Browsing Applications on iOS and Android

S. Comer and P. Leimich
University of Abertay,

Abstract

The scope of a crime can expand to another continent in a matter of seconds and nowadays there is almost no crime committed without a trace of digital evidence. According to Reiber (2014), 91% of the global population make use of a mobile device, and 82% of device usage is expended on some sort of application. It is estimated that Google processes more than 200,000 searches every minute. This statistic alone conveys just how much data is transferred worldwide, all of which leave traces of digital evidence. Many of the mobile applications available today, including Internet browsers, will request the user's permission to access their current location when in use. This geolocation data is subsequently stored and managed by that application's database files, which can be recovered from the device itself. Since the advanced functionality of devices today can be exploited to assist in crime, the need for mobile forensics is imperative, and GPS evidence and track points could hold major evidentiary value for a case.

The aim of this paper is to examine to what extent geolocation data is available from the iOS and Android operating systems. We focus on geolocation data recovered from internet browsing applications, comparing the native Safari and Browser apps with Google Chrome, downloaded on to both platforms.

All browsers were used over a period of two days at various locations to generate comparable test data for analysis.

In Android, every app manages its own information through separate SQLite files. A file of particular interest recovered from Browser was http_www.google.co.uk_0.localstorage. This SQLite file contains latitude and longitude coordinates for the places where the Google search engine had been set to use the device's location. All records were found within this file, which was as expected as no browsing history had been deleted. Exporting the latitude and longitude values into Google Maps from the records correctly revealed the location of the device at those times, with high accuracy for all but one records. While this local storage file gave the coordinates of where the Browser application updated the location, no timestamps were found within the file, thus making it difficult for a forensic investigator to use the information in a timeline. The file can, however, infer order, as location updates were stored sequentially, oldest first.

The only geolocation data that was recovered from the Google Chrome application on Android were a set of GPS coordinates for the device's last cached position, acquired from the CachedGeoposition.db SQLite database file. No GPS coordinates could be

found within the Google Chrome browser files, despite setting Google Chrome to use the device's location when the application was in use.

The Google Chrome History SQLite file contained no GPS coordinates either. However, it can still produce some more abstract, circumstantial location evidence. For example, while no coordinates were available, an entry in the SQLite database file revealed through the URLs visited and corresponding title fields that weather information was requested for the Strathclyde region from the Met Office, indicating a likelihood that the requester was in the Strathclyde area.

The iOS platform uses a single, centralised database file, consolidated.db, which is used by all apps. We expected this file to store Safari's app data, including geolocation information, but were unable to retrieve any Safari data from it.

Certain tables such as the CellLocation and WifiLocation tables, which were expected to be present within the database file did not exist, nor could these tables be found anywhere else on the iOS forensic image. The consolidated.db file simply contained two tables for compass calibration and details regarding the orientation of the device. Safari stored no data elsewhere on the system.

The iOS Chrome History SQLite file contained comparable data to the Android Chrome History SQLite file. Again, no coordinates were stored in the table but the Glasgow region searched for on Met Office was displayed, and therefore the same circumstantial location information could be inferred.

In addition to SQLite, iOS apps use property lists for data storage. Several such plists were examined, particularly GeolocationSites.plist. No coordinates were found in this plist. It merely contained one entry for imdb.com, and all that was available was a "ChallengeDate" and a "ChallengeCount”, a timestamp and access count respectively.

In conclusion, there is a considerable difference in the amount of data that is stored by the two mobile operating systems and by the internet browsing applications themselves. Both Browser and Google Chrome on the Android platform used SQLite databases to manage data. These files were application-specific SQLite files both store browsing history. Surprisingly, despite both apps being operated by Google, and both having the location updated in each visited setting, they differed fundamentally with regard to location information. Browser was able to provide highly accurate coordinates of where each update occurred whereas Google Chrome did not store these coordinates.

iOS applications use SQLite database files or property lists to manage data. While property lists are application-specific, all geolocation data is centralised in one single iOS-managed SQLite database file, which provided no valuable GPS information in this investigation. This would warrant further investigation.

Use of Netflow/IPFix Botnet Detection Tools toDetermine Placement for Autonomous VM’s

Razvan-Ioan Dinita, Andrew Moore, Adrian Winckles and George Wilson
Anglia Ruskin University

Abstract

This paper describes a novel method of autonomously detecting malicious Botnet behaviour within a Cloud datacentre, while at the same time managing Virtual Machine (VM) placement in accordance to its findings, and it presents its implementation with the Scala programming language. A key feature of this method, using output from Netflow/IPFix, both of which are capable of producing detailed network traffic logs, is its capability of detecting unusual Client behaviour through the analysis of individual data packet information. It has been implemented as a module of an Autonomous Management Distributed System (AMDS) presented in [Dinita, R. I., Wilson, G., Winckles, A., Cirstea, M., Rowsell, T. (2013)], giving it direct access to all the VMs and Hypervisors on the Cloud network. As such, another key feature is that it can have an immediate and effective impact on network security in a Botnet attack context by issuing lockout commands to every networked VM through the AMDS. A proof of concept has been developed and is currently running successfully on the authors’ test bed.

Analysis of Feodo Malware: A Complimentary Approach

Robert Burls and Dr Philip Nobles
Cranfield University

Abstract

The Feodo banking Trojan, also known as Bugat or Cridex, first seen in 2010 became prevalent in 2012. This Trojan is now reported to be reappearing in 2014. Whilst Feodo has not received the media attention of the notorious ZeuS malware and related offspring, it is, however considered to be significant enough to earn a place on the venerable abuse.ch website, which monitors important banking Trojan malware.

This paper presents the lead author's analysis of Feodo malware that was initially carried out for a major European bank. It examines versions of Feodo that are shown to be current and takes into consideration operating system state changes including Windows Registry and file system changes on both Windows XP and Windows 7 operating systems.

This complimentary analysis demonstrates that Feodo variants present similar forensic footprints although the network behaviour differs between the two variants, which may mislead if network-based signature analysis is solely relied upon. Our findings are unambiguous in confirming the presence of the malware on the operating systems mentioned above.

There are well documented examples on the functionality of Feodo. This paper does not seek to describe the malware, to reverse engineer it or to emulate previous research but complement previous work and to assist the forensic investigator in detecting Feodo malware on infected Windows XP and Windows 7 computers using a number of tools. The paper is structured as follows: Section 1 introduces the Feodo Trojan and malware analysis. Section 2, covers background work and gives an overview of Feodo functionality including naming conventions used for the malware. Section 3 considers the tools and methodology we have used to carry out this study. Virtualisation technology was chosen to test and examine the malware on the infected operating systems. The work was validated using an automated malware analyser. We also consider the ethical issues of our study. Section 4 discusses the results of the examinations including the common attributes. We present our summary in Section 5. Section 6 considers the legal implications of Feodo distribution with regard to the United Kingdom's Computer Misuse Act 1990 and future work is discussed in Section 7.

This paper presents instruction on how modern malware behaves on infected host operating systems and how such malware maybe identified and analysed. The paper highlights the advantage of complimentary analysis techniques.

The Cyber Security CSI Effect in Bollywood

Pulkit Vohra, Roma Gandhi and Harjinder Singh Lallie
University of Warwick

Abstract

The term “CSI effect” is derived from the popular American TV show CSI: Crime Scene Investigation. Some of the concepts explained in the TV serial has influenced the general public in terms of what they understand about the capabilities, technical boundaries and limitations of Cyber security, digital forensics, forensic science and information technology in general. The CSI effect creates unreasonable expectations on the part of jurors and the public and can have particularly adverse effects particularly in trials where the jury and even judges fail to understand technological concepts.

Hollywood and Bollywood use a range of techniques to dramatize cyber security concepts. Occasionally, impossible concepts are made to seem and feel possible whereas simple concepts are made to seem overly complex. We demonstrate this phenomena by referring to a number of films from the Bollywood - largest film industry in the world from a country which is fast growing to become a global IT powerhouse. In this paper we highlight a number of features of this phenomena and put them into the context of cyber security, we consider for instance the way in which some movie portrayals reinforce worrying views of the ‘insecurity’ of security and also the manner in which near impossible concepts are portrayed to seem real to the viewing public.

Keywords: Bollywood, Cyber Security, CSI Effect

Forensic Implications of Portable Operating Systems

Charles Frewin and Dr Morris
Centre for Forensic Computing, Cranfield University

Abstract

The development of portable technologies has made mobile computing publically available for mainstream use. The increased consumerisation of the IT industry has prompted a growing trend in the use of portable operating systems. Employers and industry have also begun to realise the cost and productivity benefits that accompany this trend. The speed and relatively low cost of hardware coupled with the availability of robust operating systems, which can be installed and run from a portable USB drive is providing further incentive to adopt this new technology. This portability offers greater freedom and flexibility in how and where users can work, as it allows the operating system to be run on any compatible host computer. These powerful devices may also be attractive to users who seek to perform unlawful activities. Historically digital investigations have centred around computers; leaving the seemingly innocuous USB device to be overlooked until later on in the case. Multiple storage devices are being seized more commonly, and the adage of them being used to only store files is rapidly becoming outdated.

This paper highlights the requirements for analysts to understand what constitutes a portable operating system. How these devices function, where and what they have been used for. This paper also investigates different portable devices, how they are created, the technologies involved and how their impact can be examined when they interact with the environment they are connected to. The aim of this paper is to provide a forensic examiner with a means of establishing the presence and usage of these devices, by examining the evidential value of the artefacts created as a result of the use of these types of technology.

A Strategic Human Resource Management Model to Develop a High Performance Work System for Cyber Crimes Investigators Within UAE Police Force

Jassem I Al Mansoori, Graham Benmore and Margaret Ross
Southampton Solent University

Abstract

Strategic Human Resources Management (SHRM) in the UAE has evolved out, as elsewhere, of the need to confront the ever-increasing challenges. These challenges emanate basically from a globalised world order, which manifests itself in digital and technological problems, terrorism, credit card fraud, human trafficking, money laundering, computer hacking and economic crises, to mention but a few. The realisation by the Ministry of Interior of these disastrous implications and negative outcomes has prompted the importance of the human resources management as a drive for building a goal-oriented ministry. This objective will only be possible through building a broad degree of involvement, coordination and strong commitment by the various relevant officials for reaching consensus of action. It was decided that to make the suggestions realistic and workable, which were based on several stages of quantitative and qualitative research at UAE police and best practice literature, that they must be presented and discussed by top management in the Ministry of Interior and other officials whose work is relevant.

The surveys, field visits and interviews have included the following ministries and departments: The Ministry of Interior (the General Inspector's Office, the General Manager for Human Resource, the Deputy General Manager in H.H. the Minister's Office, the Dubai police H.Q.), the Ministry Of Justice, the Emirates Telecommunication Corporation and the Ministry Of High Education and Scientific Research.

This final stage of the research has facilitated the development of abridged and unified suggestions, which this paper seeks to present. The proposed model is based on the view of the senior participants that unity of effort and coordinated action at the federal level are crucial.

The model discusses the following five central features considered crucial to capacity building for the working force and very specifically for the development of investigators' work performance to confront and detect globalisation induced and unprecedented cyber crimes:

1. The establishment of a High National Committee for combating and detecting electronic crimes to fulfil various roles, particularly the preparation of a strategic plan and the establishment of specialised teams to combat electronic crimes.
2. The establishment of a central Security Institute specialised in combating electronic crimes.
3. Activation of judicial corporation in order to strengthen the efficacy of international agreements on electronic crimes and criminal arrests.
4. Establishment of a National Information Center for strengthening strategic partnership, exchange of information relevant to internet crimes and identifying internet hackers at the regional and international levels.
5. Creation of an organisation unit, as part of the Ministry's organisational structure and within the framework of the federal efforts to combat electronic crimes.

Education and Privacy:
PIN and Passphrase Selection Strategies

David Harley
ESET Senior Research Fellow

Abstract

Looking through my mail today I saw reports of no less than four major security breaches concerned with the theft of user records and the disclosure of credentials. It's unlikely that any single factor authentication solution guarantees absolute privacy, least of all the traditional static password. And there's little the end user can do to protect himself against exposure where service providers fail to implement the most elementary precautions properly or at all except to avoid using the service. Nevertheless sometimes only the humble PIN, password or passphrase stands between the end user and the hacker.

Yet most advice to those customers goes no further than 'Don't use "password" or "123456"' and the media are apt to substitute lists of the top umpteen poor passwords for real, useful information. We can at least offer better (basic) information on how authentication works, encourage users to take advantage of multi-factor authentication where it's available, and urge service providers to take their responsibilities towards their customers' data more seriously. But is it possible to help users to help themselves without understanding *why* they do what they do, so as to make it *easier* for the user to make it *harder* for the attacker?

In the hope of reaching this understanding, we will consider some of the most critical factors that govern passphrase and PIN selection strategies:

- Limitations imposed by sites, services, and user policies
- Mnemonics and memorization strategies
- Ergonomics and hardware.

We will ask whether there is a need to re-examine the advice we give to end users after analysis of high-profile passphrase and PIN breaches and suggest some alternative approaches. Drawing on a number of case studies providing data from password breaches and PIN usage studies, and attempt analysis of typically stereotyped passcodes that goes beyond simple lists of 'bad' passwords. We examine the main behavioural factors that influence password and PIN selection strategy, especially ergonomic factors and memorization strategies.

We assess the validity of commonly recommended strategies in a diversity of contexts and consider recommendations based on the findings of this analysis of common strategies, placed into the context of more general mixed-character passwords and passphrases, and offer recommendations for more realistic approaches to passcode authentication. The hope is that when put into the corporate context, they will provide a starting point for security managers and administrators responsible for the protection by authentication education and policy of end users and customers.

Invited Keynote Presentation
The Legacy of 2Centre

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

This new centre recognises the work being completed by staff in the University in the area of Cybercrime Forensics; which has included hosting the annual International Conferences on Cybercrime Forensics Education and Training (CFET) and the work leading the €1 million EU funded ECENTRE (England's Cybercrime Centre of Excellence Network for Training Research and Education) project in association with the College of Policing, PCeU, ACPO eCrime Training, ten UK universities and four companies (n-Gate Ltd, Technology Risk Ltd, First Cyber Security Ltd, Evidence Talks Ltd).

Sponsor – College of Policing

The COP (formally CENTREX and NPIA) provide specialist training and support to the 43 national police forces in the UK. COP 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

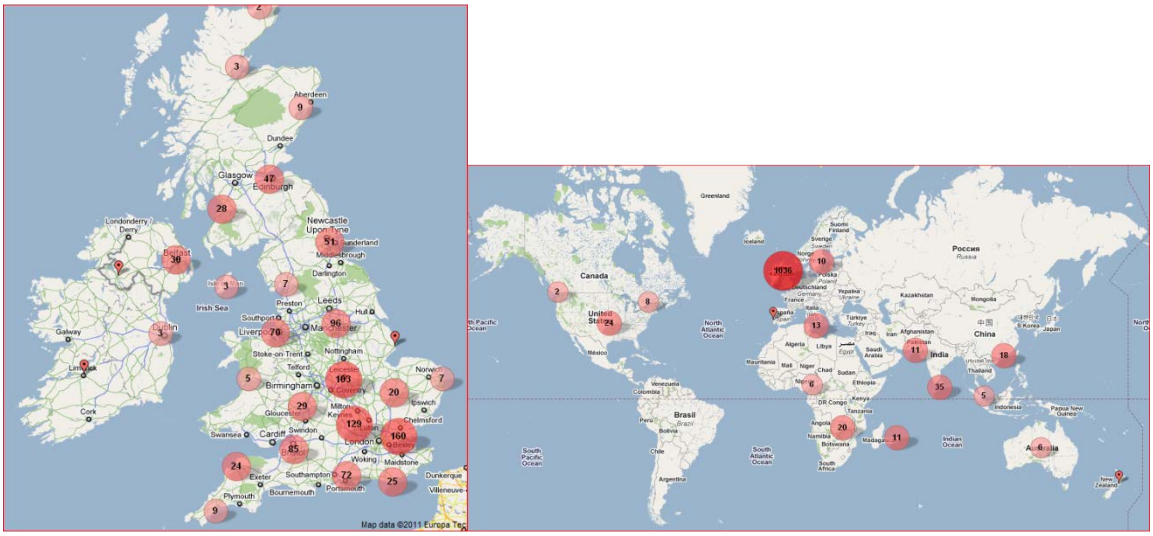
Provincial post-secondary institute, founded under College & Institute Act, for Justice & Public Safety education in 1978, by Dr. Patrick McGeer, Minister of Education. Its mission is to provide Innovative education and training for those who make communities safe. Its vision is to be a world leader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

bcs
The
Chartered
Institute
for IT

Cybercrime Forensics
Specialist Group

Established in 2008, the SG now has over 1620 members in 55 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/

Copyright Statement

NOTES

NOTES