Institution: Edinburgh Napier University

Unit of Assessment: 11: Computer Science and Informatics

Title of case study: Protecting Employees, Children and Sensitive Data using Innovative Approaches to Cyber Security

Period when the underpinning research was undertaken: March 2005 to May 2020

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Professor Bill Buchanan	**Professor** *(formally senior lecturer)*	September 1989-present
Dr Owen Lo	**Research Fellow** *(formally RA)*	September 2012-present
Dr Jamie Graves	**Research Fellow** *(formally and RA)*	August 2008-August 2010 February 2012-January 2013
Dr Gordon Russell	**Associate Professor**	August 1995-present
Bruce Ramsay	**Lecturer** *(formally Research Fellow)*	March 2014-April 2020
Richard Macfarlane	**Associate Prof** *(formally lecturer)*	March 2009-present
Dr Zhiyuan Tan	**Lecturer**	August 2016-present

Period when the claimed impact occurred: August 2015 to Sept 2020

Is this case study continued from a case study submitted in 2014? N

1. Summary of the impact (indicative maximum 100 words)

Research at Edinburgh Napier University has led to the development of technology that can rapidly detect cybercrime. This led to the creation of two successful spin-out companies (ZoneFox, and Cyan Forensics). The AI-driven insider threat analysis software developed by ZoneFox has been installed by the Scottish government for 15,000 end-points and the company was acquired by Fortinet for GBP28million. Cyan Forensics products enable faster detection of illegal online content and are being used by law enforcement agencies in the UK and internationally in cases of child abuse and sexual exploitation. The company has received GBP3.5million investment.

2. Underpinning research (indicative maximum 500 words)

Cyber-crime is a growing challenge to law enforcement agencies across the globe. Crimes such as digital fraud and digital contraband (such as child pornography where images are moved across borders to jurisdictions where they are illegal) cause significant harm and must be solved in a timely manner. Research led by Professor Bill Buchanan has enabled the creation of tools that help reduce the time it takes to investigate digital devices and provide creditable digital forensics evidence.

From 2005-2008, Prof Bill Buchanan and Dr Jamie Graves, as part of Graves' PhD, developed a novel bio-inspired method of mapping interrupt calls on a computer in order to detect threats. This led to the funding of a Proof of Concept **[P1]**. Two patents followed in 2014: US8887274B2 **[O1]** and EP1347366A1.

The patents captured the core research: defining activity footprints as a 'digital DNA' sequence, which can be used with a new matching algorithm (BLAST DNA) to determine the probability of a sequence match to a malicious event, significantly outperforming existing signature-based methods. This provided particularly useful in detecting insider threats such as copying source-code to a USB device.

From 2014-2016, Prof Bill Buchanan led research involving Dr Phil Penrose, Bruce Ramsay and Rich Macfarlane to address a significant challenge within digital investigations for law enforcement: the increased workload associated with digital investigations in order to identify presence of encrypted content. This research – supported by four grants **[P2][P3][P4][P5]** – made a step change in digital forensics by applying novel techniques based on data entropy to differentiate between compressed and encrypted fragments **[O2]**. This was applied in the detection of contraband within disk systems using digital fragments of data **[O3]**. The work demonstrated at least 100 times speed-up in finding contraband content on a disk. This allows law enforcement to quickly detect the presence of contraband content, and thus seize a device for further investigation. This research **[O3]** also showed that the digital fragment method could successfully detect digital contraband on large capacity disks, working in conjunction with Police Scotland on a real-life criminal investigation. Its key contribution was in identifying the difference between compressed files and encrypted files by measuring the entropy of a fragment. The new methods resulting from the research that use digital fragments to identify illegal contraband and which generated a patent application in 2017 **[O7]**.

The team then progressed this work by including triage methods into the discovery of encryption keys within memory **[O4, O5]**. Key contributions include being the first to detect the presence of ChaCha20 encryption keys in running memory (one of the most popular encryption methods used in secure communications), and identifying a major vulnerability within tools such as OpenSSL. Further research focused on the presence of digital forensics information emitted from devices thought side channels (and where a side channel is the leakage of information from a device through unwanted transmission) **[O6][P7][P8]**. This work was the first to discover a side channel vulnerability within the PRESENT light-weight cryptography method (and which is one of the most popular standards defined for light-weight cryptography) and was part of an industrial research collaboration with Keysight **[P6]**. The work analysed the presence of electrical noise generated within an IoT device.

3. References to the research (indicative maximum of six references)

[O1] Buchanan, W. J., Graves, J. R., & Bose, N. (2014). U.S. Patent No. 8,887,274. Washington, DC: U.S. Patent and Trademark Office. World patent: WO2010029346A1. https://patentimages.storage.googleapis.com/cd/aa/3a/369c4f7c7a0093/US8887274.pdf
[O2] Penrose, P., Macfarlane, R., & Buchanan, W. J. (2013). Approaches to the classification of high entropy file fragments. Digital Investigation, 10(4), 372-384. https://www.researchgate.net/profile/William_Buchanan2/publication/259164873_Approaches_to_the_classification_of_high_entropy_file_fragments/links/5a53bc490f7e9bbc10570825/Approaches-to-the-classification-of-high-entropy-file-fragments.pdf
[O3] Penrose, P., Buchanan, W. J., & Macfarlane, R. (2015). Fast contraband detection in large capacity disk drives. Digital Investigation, 12, S22-S29. https://www.sciencedirect.com/science/article/pii/S1742287615000080 **[Submitted to REF2]**
[O4] McLaren, P., Buchanan, W. J., Russell, G., & Tan, Z. (2019). Deriving ChaCha20 key streams from targeted memory analysis. Journal of Information Security and Applications, 48, 102372. https://arxiv.org/pdf/1907.11941
[O5] McLaren, P., Russell, G., Buchanan, W. J., & Tan, Z. (2019). Decrypting live SSH traffic in virtual environments. Digital Investigation, 29, 109-117. https://arxiv.org/pdf/1907.10835
[O6] Lo, O., Buchanan, W. J., & Carson, D. (2017). Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA). Journal of Cyber Security Technology, 1(2), 88-107. https://www.tandfonline.com/doi/pdf/10.1080/23742917.2016.1231523
[O7] William Johnston Buchanan, Owen Chin Wai LO, Philip Penrose, Richard MacFarlane, Ian Stevenson, Bruce Ramsey Method for reducing false-positives for identification of digital content, World patent: WO2018185455A1, European patent: EP3607467A1 https://patents.google.com/patent/EP3607467A1/en

Indicators of quality: Rigorous peer review. International reference points.

This research and its exploitation has been funded through the following grants:

[P1] DigitalDNA. Funder: Scottish Enterprise. Sep 2008 - Aug 2010. Value: £215,000.
[P2] Fragment Finder, Proof of Concept Fund. Funder: Scottish Enterprise. Mar 2015 – Jan 2016. Value: £230,042.
[P3] Bare Metal Forensics - Pattern Analysis Heuristics - Data Analysis, Funder: Data Lab, Jan 2016 - Jan 2017. Value: £64,884.
[P4] SBRI - Fragment Finder. Funder: Innovate UK. Feb 2016 - Jun 2016. Value: £37,718.
[P5] Dynamic Forensics Evaluation and Training (DFET). Funder: European Programmes. Jan 2014 - Jan 2016. Value: £271,071.
[P6] IoT Hardware Security Test Framework. Funder: CENSIS, Keysight. Nov 2017 - Oct 2018. Value: £81,753.
[P7] Memcrypt, High Growth Spin-out Programme (HGSP). Funder: Scottish Enterprise. PI: WJ Buchanan. Others: Owen Lo, Gordon Russell, Peter McLaren, Sep 2020 - 31 Mar 2021. Value: £179,545
[P8] MemCrypt, CyberASAP Programme (Stage 2), Funder: Innovate UK. PI: WJ Buchanan. Others: Owen Lo, Gordon Russell, Sept 2020 – March 2021. Value: £80,612.

4. Details of the impact (indicative maximum 750 words)

Our research outlined above has resulted in two highly successful spin-outs, and has created impact across a number of key cybersecurity areas.

Cyber security:
Our Digital DNA work created a novel methodology for detecting any type of computer activity using DNA matching methods. Following completion of Grave's PhD, Proof-of-Concept funding from Scottish Enterprise was awarded **[P1]**. As a result Jamie Graves and Bill Buchanan co-founded Inquisitive Systems **[C15]**. This company was then rebranded as ZoneFox.

The main application area was in the protection digital assets, especially around IP theft **[C1]** and in Artificial Intelligence applied to Cyber Security. Graves was CEO of ZoneFox, until its acquisition by Fortinet in 2018.

ZoneFox initially received angel investment of over GPB2.5million. The company integrated its work, with a major contract, into Wolfson Microelectronics, which detects the movement of digital assets. The company received several awards for innovation and enterprise. It has developed an advanced data protection system, which is being used across a number of organisations, to detect IP theft events, including with Rockstar, Wolfson, Craneware and Cirrus Logic **[C2]**.

In 2017, ZoneFox received another GBP3.6million in funding and grew to a staff count of 30 with offices in Edinburgh and London **[C3]**. The company won industry awards including International Contribution to Cyber-Security and the overall Champion of Champions at the Scottish Cyber Security awards in 2016 **[C4]**, winner of CIR Risk Management Award for Cyber Security Product of the Year in 2018 **[C5]** and was included in the Real Business Top 50 most disruptive UK companies in 2017 **[C6]**. In 2018, it was acquired by Fortinet for GBP28million. In 2019, ZoneFox software was selected to protect all the Scottish Government employees and data across 15,000 endpoints **[C12]**.

In Dec 2020, Edinburgh Napier University was awarded a prestigious Royal Society Entrepreneur in Residence position for Dr Jamie Graves. His role will be to encourage entrepreneurial activities and help turn leading research and ideas into commercial impact and success.

Digital Forensics

A Scottish Enterprise Proof of Concept grant **[P2]**, followed by a Home Office SBRI grant **[P4]** supported the commercialisation of the digital triage research, which had built on the earlier work on digital fragments. This led to the creation of the spin out company, Cyan Forensics, in 2016. Cyan Forensics' focus has been on faster triage of digital data and in the detection of contraband content, and which uses the core methods developed within the Napier research **[O2][O3]**. Bruce Ramsay, who was a research fellow on the Napier team, is now the company's Chief Technical Officer. According to Cyan Forensics CEO Ian Stephenson: "*A core part of the success of the company has been translation of the core research work undertaken within the university of triage methods. The scientific methods and the evaluation applied has since been used to build the core of the IP within the company, and is a fundamental part of our product range.*" **[C11]**. The company now works with UK police forces on real-life investigations, using the methods developed through the research.

By 2020, the company had received over GBP3.5million in cumulative equity and grants, including GBP900,000 in an investment round led by Mercia Fund Managers in 2018 and a further GBP1.3million in 2019 **[C7]**.

Cyan Forensics won the PitchGovTech event in Paris as part of GovTech Summit 2019, which highlights technologies across Europe that can have a major impact on the public sector **[C8]**. The company also received a Cybersecurity award in the same year for "Best Cyber Breakthrough" **[C13]**.

In 2019, Cyan Forensics partnered with the Home Office and UK-based companies Qumodo and Vigil AI to produce new tools to improve the capability of the Child Abuse Image Database (CAID) **[C9]**. These included: a fast-forensic tool to rapidly analyse seized devices and find images already known to law enforcement; an image categorisation algorithm to assist officers to identify and categorise the severity of illegal imagery; and a capability to detect images with matching scenes to help identify children in indecent images in order to safeguard victims [C9]. Together, the tools speed up investigations of online child abuse and limit the number of indecent images of children that police officers have to view. The then Home Secretary Sajid Javid called the technology "*game-changing"* and said that was *"vital in the fight against online child abusers.*" **[C9]**.

Cyan Forensics now works with Police Forces across the UK in time-critical Child Sexual Exploitation and Counter Terrorism cases, and their product has been proven to provide digital evidence between 20 and 100 times faster than was previously possible **[C14]**.

Cyan Forensics' products are also in use with law enforcement agencies in the USA. In 2019, the company established a partnership with the National Centre for Missing and Exploited Children (NCMEC) in Virginia **[C10]**. NCMEC's CyberTipline is a centralized reporting system for child sexual exploitation and receives reports from the public and internet companies. This is then distributed to agencies such as the FBI, Homeland Security, the Secret Service, the US Military, Internet Crimes Against Children Task Forces (ICACs), and law enforcement in over 110 countries. John Clark, President and CEO of NCMEC, said: "*Timing is often critical in these cases, and we're excited at the prospect of new technology that could provide faster access to information that will help rescue children from abuse. Cyan Forensics' technology has the power to make a big impact in the fight against online child sexual abuse imagery*." **[C10]**.

The technology is also being used to identify harmful content online. Company CEO Ian Stephenson said: "*We are also taking the same technology we have deployed in Law Enforcement and applying it to Online Safety, where we are at the heart of international efforts to block and remove child abuse and extreme terrorist content from social media sites*." **[C11]**.

5. Sources to corroborate the impact (indicative maximum of 10 references)

[C1] Screenshot from PR Newswire. ZoneFox Develops World Leading Insider Threat Detection Monitoring [Internet]. [cited 2017 May 30]. Cybersecurity01.png. Available from: http://www.prnewswire.c...nitoring-550409531.html

[C2] PDF document on Cirrus Case Study. Cybersecurity02.pdf. https://www.dropbox.com/s/9r7l7a5ths9b4ah/zf_casestudy_cirrus-logic.pdf

[C3] PDF document on Investigation of a data theft The state of security. [cited 2018 Apr 3]; cybersecurity03.pdf Available from: https://www.dropbox.com/s/y0uepq4s1p5zi99/cybersecurity03.pdf?dl=0

[C4] Screenshot from Cyber Crime Champions Honoured At Inaugural Awards [Internet]. [cited 2018 Apr 3]. cybersecurity04.png Available from: https://www.holyroodpr.co.uk/sbrc-cyber-awards/

[C5] Screenshot from Cyber Security Product of the Year from CIR Risk Management [Internet]. [cited 2018 Apr 3]. cybersecurity05.png Available from: https://www.cirmagazine.com/riskmanagementawards/media.php

[C6] Screenshot from The Future 50: The 50 most disruptive UK companies [Internet]. [cited 2018 Apr 3]. cybersecurity06.png Available from: https://realbusiness.co...e-uk-companies-2017/10/

[C7] Screenshot from Edinburgh tech start-up Cyan Forensics gets £1.3m funding injection, cybersecurity07.png https://www.scotsman.com/future-scotland/innovators/edinburgh-tech-start-cyan-forensics-gets-ps13m-funding-injection-1400267

[C8] Screenshot from University Spin-out - Cyan Forensics - Wins at GovTech Summit 2019, https://www.scotlandis.com/blog/edinburgh-tech-start-up-wins-pan-european-pitching-competition/, cybersecurity08.png 18 Nov 2019.

[C9] Screenshot from Pioneering new tools to be rolled out in fight against child abusers, cybersecurity09.png https://www.gov.uk/government/news/pioneering-new-tools-to-be-rolled-out-in-fight-against-child-abusers

[C10] Screenshot from UK-based Cyan Forensics partners with major US nonprofit to stop child sexual abuse, cybersecurity10.png https://www.eu-startups.com/2019/08/uk-based-cyan-forensics-partners-with-major-us-nonprofit-to-stop-child-sexual-abuse/

[C11] PDF Letter from Cyan Forensics CEO, Ian Stephenson, cybersecurity11.pdf https://www.dropbox.com/s/34umtqiqkjh11fj/2020-12-03%20Cyan%20Forensics%20REF.pdf?dl=0

[C12] Screenshot from ZoneFox wins major Scottish government security contract, cybersecurity12.png https://tech.newstatesman.com/security/zonefox-scottish-government-contract

[C13] Screenshot from Best Cyber Breakthrough, Scottish Cyber Awards. 2019, cybersecurity13.png https://www.napier.ac.uk/about-us/news/scottish-cyber-awards-2019

[C14] Screenshot from Disk Test Evaluation, cybersecurity14.png

[C15] PDF Letter from Jamie Graves, co-founder Inquisitive Systems, cybersecurity15.pdf