Research Assessment Exercise 2020
Impact Case Study

University: The University of Hong Kong (HKU)
Unit of Assessment (UoA): UoA 13, computer studies/science (incl. information technology)

Title of case study: Cyber Security and Digital Forensics and their Applications

(1) Summary of the impact

Since 2000, the Department of Computer Science has been conducting extensive research in cybersecurity. In addition to its highly rated research output, the department has been actively applying its expertise to the security needs of industry and wider society. […] Among other examples, the department's research contributed to the first worldwide criminal conviction of copyright infringement using BitTorrent in 2005 […]. It also led indirectly to the shutdown of a major piracy content sharing site, MegaUpload, by the FBI in 2012. In addition, the department's work in digital forensics has featured in numerous court cases in HK and the US, helping to bring cybercriminals to justice. This work helps to maintain the rule of law in the digital era, and creates a more secure environment for traditional industries employing advanced information technology and undergoing digital transformation.

(2) Underpinning research

The department started its theoretical work on cryptographic library implementations and applications in 1999 (HKCS Database Conference 1999).[…] That eventually led the department to open up a new research area: cybercrime modeling and digital forensics. The team defined a research roadmap in this field and has dedicated its efforts during the past two decades to building on its pioneering research. […]

[…]The department is one of the pioneers in this research area and collaborates extensively with experts around the world in similar fields. As a recent example, the department published a joint work with a scholar at King's College, London which quantified the likelihood that a prosecutor could prove beyond doubt that a defendant had indeed downloaded illegal material (e.g., child pornography) from the Internet (Forensic Sciences Research 2016) [3.3].

[…]In 2008, the department developed the world's first cybercrime model, using a Bayesian network in a criminal case which pioneered the practice of file sharing using BitTorrent (International Federation for Information Processing (IFIP) 2008, Association of Digital Forensics, Security and Law (ADFSL) 2012). This work attracted the attention of academics worldwide, and researchers at King's College, London have since further developed this technique.

In addition, the department has done extensive work in monitoring and detecting […]copyright infringement activities on the Internet. […]Recently, with the advent of the Internet-of-Things (IOT) with its associated security challenges, this research has been extended to threat analysis of network-connected control systems (e.g., elevators) (IFIP 2016 & 2017). Our paper "Threat Analysis of an Elevator Control System" has been downloaded more than 4,000 times since its publication in November 2017 (https://www.researchgate.net/publication/321172318_THREAT_ANALYSIS_OF_AN_ELEVATOR_CONTROL_SYSTEM).

The department has also studied data privacy protection problems, particularly in the context of procedural justice. It worked on protecting digital legal professional privilege (LPP) data in 2008

(SADFE 2008), and subsequently published a research paper (which received the best paper award) and a journal paper in 2011 and 2013 respectively (SADFE 2011, IFS 2013 [3.1]).

(3) References to the research

[3.1] Jiang Z.L., Fang J.B., Law Y.W., Lai P.K.Y., Ieong R.S.C., Kwan Y.K., Chow K.P., Hui C.K., Yiu S.M. and Pun K. H., Maintaining hard disk integrity with digital legal professional privilege (LPP) data, IEEE Transactions on Information Forensics and Security (IEEE IFS). 2013, 8(5): p.821-828. (Publication Date: April 2013).

[3.2] […]

[3.3] R. E. Overill and K.P. Chow, An approach to quantifying the plausibility of the inadvertent download defence, Forensic Sciences Research (Dec 2016), Vol. 1, No. 1, pp 28-32. Taylor & Francis. (PubMed Central indexing, an archive of biomedical and life sciences journals at the US National Institutes of Health's National Library of Medicine (NIH/NLM).

(4) Details of the impact

[4.1] […]

[4.2] **Develop a scientific and practical approach to digital forensics**. Besides establishing the theoretical foundations of digital forensics in its research, the department has also provided practical support to the judicial system in multiple ways. […]

[4.3] **Promote data privacy**. Motivated by real-world investigations, our team has devised solutions for ensuring the integrity of digital evidence without sacrificing data privacy. We proposed a practical solution for maintaining the integrity of digital devices, particularly hard disks, while protecting the data that is supposed to be only disclosed to a defendant's legal advisor (known as legal professional privilege (LPP) data in Common Law jurisdictions[…]. LPP is an important practice that helps to uphold the Rule of Law. The department's work offers a practical protocol for extending LPP to digital evidence [5.6].

[4.4] **Productize cyber security**. In 2016, the department developed and rolled out a product, "SHIELD" (Smart Hacking and Intrusion Entrapment with Lawful Dectection), to the market.[…] This is crucial for allowing traditional industries to undergo digital transformation and adopt information technology in their businesses, without heavy investment in equipment and expertise to protect themselves against cyberattacks. […]

[4.5] **Train cybersecurity experts**. Since 2010, the department's research center has trained 11 PhD and four MPhil graduates[…] In addition to educating people within the University, the department has also played a leading role in engaging the community and raising the level of cybersecurity knowledge and skills across industry in general. […]

[4.6] **Commercialize**. […]It promotes awareness of cybersecurity among the general public, and extends the department's work and expertise through commercial offerings. In the long term, its work will improve HK's business environment and increase its competitiveness. […]

(5) Sources to corroborate the impact

[5.1] [5.1] CHAN P.S.V., Chow K.P., Kwan Y.K., Fong G., Hui M. and Tang J., An Exploratory Profiling Study of Online Auction Fraudsters, Tenth Annual IFIP WG 11.9 International Conference on Digital Forensics, 8-10 January 2014, Vienna, Austria. USA, Springer.

[5.2] CHAN C.B., Chow K.P., CHAN P.S.V. and KWAN Y.K., The Cloud Storage Ecosystem - A New Business Model for Internet Piracy?, Twelfth Annual IFIP WG 11.9 International Conference on Digital Forensics, 4-6 January 2016, New Delhi, India. USA, Springer, 2016, 237-255.

[5.3][…]

[5.4][…]

[5.5] M. Kwan, R.E. Overill, K.P. Chow, J.A.M. Silomon, H. Tse, F. Law & P. Lai, Evaluation of Evidence in Internet Auction Fraud Investigations, Proc.6th Annual IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, 3-6 January 2010, Advances in Digital Forensics VI, Ch.7, pp.95-106, Springer (2010).

[5.6][…]

[5.7][…]

[5.8][…]

[5.9][…]

[5.10][…]