Institution: University of East London (UEL)

Unit of Assessment: 11 Computer Science and Informatics

Title of case study: Cybersecurity and cybercrime prevention

Period when the underpinning research was undertaken: 2013 – 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:**
Dr Paolo Falcarin	Reader in Computer Science	2010 – present
Dr Ameer Al-Nemrat	Reader in Cybersecurity	2008 – present

Period when the claimed impact occurred: 2014 – 2020

Is this case study continued from a case study submitted in 2014? No

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

As the world increasingly relies on the internet and digital services, the public are more vulnerable to cybercrime.

Dr Ameer Al-Nemrat has developed a database search methodology to alleviate pressure on investigative teams. His research has also revealed the relationship between progression of protective legislation, cybersecurity technologies and personal education.

Dr Paolo Falcarin contributed to the development of the ASPIRE toolchain, a first open-source toolset of native code obfuscators and protections for preventing software piracy on mobile apps, which has been turned into commercial products by companies such as Thales and Kudelski to combat cyberattacks against companies.

2. Underpinning research (533, indicative maximum 500 words)

Database algorithm and cybervictimisation;

The UK's CAID has grown exponentially, containing over 13 million images and processing the sheer quantity of new and duplicated images is becoming an increasing burden to investigative teams. Law enforcement branches used two primary methods to handle the images: 1) the pattern-matching technique, which identifies and matches images based on key vectors; or 2) matching hash sets, which calculates a 'fingerprint' for an image based on perceptual details. However, the abundancy of photo-editing software increased the variation of images that can be produced from a single photo resulting in an increased unreliability of the matching systems. As a consequence, investigating teams had to manually catalogue many of the images to fulfil UK legal requirements.

Dr Al-Nemrat addressed this problem by modelling a statistical algorithm which can automatically identify and cluster copies of the same image from different sources. Converting images into two different hash values (MD5 and SHA-1) to cluster similar images and then collating different statistical analysis tools, the algorithm allows investigative organisations to handle large quantities of images in a short period of time with greater accuracy and reliability than previous methods by constraining the search to a subset based on sound statistical principles. **(R1)**

Al-Nemrat's research pointed to strong associations between online activity and time spent online and cybervictimisation, and that legislative measures did not sufficiently address the problem. The work supported the development of a comprehensive Incident Response Framework (IRF), which informed legal authorities and victims' service provision **(R2)**.

The ASPIRE Toolchain;

The latest BSA Global Software Piracy Study shows the continuous worldwide presence of online piracy of digital contents, amounting to $46.3 billion in losses due to software piracy. The team, led by Falcarin, conducted research contributing to the creation of the first open-source toolchain of obfuscators and software protections for native code in Android apps within the ASPIRE research project.

Falcarin led the development, together with Ghent University, of the ASPIRE renewability framework (plugin of the ASPIRE toolchain) for implementing dynamic updates of binary code on Android apps **(R3)** and advanced features for making other types of protection renewable and combinable; the use of renewable and diversified protections, reducing the window of opportunity for generating income from an attack, aims at increasing the effort needed to identify and manually exploit successful attack vectors, mitigating the risk of automated scale-up exploitation.

Falcarin worked on modelling Man-At-The-End (MATE) attacks on industry applications, showing different attacks on Android apps developed by three companies **(R4)**. This work helped the companies in understanding which attack paths were easier for the attackers, helping them to focus on improving the protections involved.

Falcarin helped tackling the open problem of security assessment of protected apps, applying the open-coding qualitative analysis to reports written by penetration testers from companies in the ASPIRE project: this work helped companies understanding the dependencies and conflicts between different protections **(R5)**. As a result, a public challenge was organised, where the participants needed to find a secret key hidden in eight versions of an application, each protected with a different subset of protections: the winner only hacked five of them, and two of the three non-hacked versions contained were protected by the code renewability framework. **(R6)**

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

R1. Sarantinos, Nikolaos; Al-Nemrat, Ameer; Naeem, Usman, "Statistical Sampling Approach to Investigate Child Pornography Cases," Fourth IEEE Cybercrime and Trustworthy Computing Workshop (CTC), pp.22-29, Nov. 2013; https://doi.org/10.1109/CTC.2013.14

R2. Al-Nemrat, Ameer and Benzaid, Chafika (2015) 'Cybercrime Profiling: Decision-Tree Induction, Examining Perceptions of Internet Risk and Cybercrime Victimisation', in 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom), Helsinki, Finland, Aug. 2015, pp. 1380-1385, https://doi.org/10.1109/Trustcom.2015.534

R3. B Abrath, B Coppens, J Van den Broeck, B Wyseur, A Cabutto, P Falcarin, B De Sutter: Code Renewability for Native Software Protection. ACM Transactions On Privacy and Security, v 23(4), 2020, https://dl.acm.org/doi/10.1145/3404891

R4. C Basile, D Canavese, L Regano, P Falcarin, B De Sutter: A Metamodel for Software Protections and Reverse Engineering Attacks. Journal of Systems and Software, Elsevier, 2019, https://doi.org/10.1016/j.jss.2018.12.025

R5. Mariano Ceccato, Paolo Tonella, Cataldo Basile, Bart Coppens, Bjorn De Sutter, Paolo Falcarin, and Marco Torchiano: How Professional Hackers Understand Protected Code while Performing Attack Tasks. In Proceedings of the 25th IEEE International Conference on

Program Comprehension (ICPC-2017), Best paper award and ACM Distinguished paper award. http://doi.org/10.1109/ICPC.2017.2

R6. M Ceccato, P Tonella, C Basile, P Falcarin, M Torchiano, B Coppens, B De Sutter: Understanding the Behaviour of Hackers while Performing Attack Tasks in a Professional Setting and in a Public Challenge. Empirical Software Engineering, 2018, https://doi.org/10.1007/s10664-018-9625-6

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

Impact on performance of existing business

The Code Renewability framework research **(R1)** and software **(S4)** have been applied by Kudelski (market-leader in security services for digital TV) for their production architecture to protect their video-players. According to a Senior Product Manager at Kudelski IoT, since 2017 the has increased the security of their apps on Android devices without penalizing performances:

“We have been able to adapt the ASPIRE software to our platform and the contribution of Paolo’s team helped us addressing the challenge of dynamically updating crypto-libraries in our digital TV products, deployed across the globe in around 200 million devices today” **(S1)**.

Thales has used the Code Renewability framework together with a trusted enclave for an early release in 2017 of the Alicem application, used by the French government to authenticate citizens through their mobile phones **(S2)**.

Kudelski and Thales used the result of our qualitative analysis **(R5)** on their tiger-team reports to improve the security of their products, and Thales also applied the attack modelling methodology **(R4)** for their own applications **(S2).**

Impact on business technology

The research on combining protections in the ASPIRE Toolchain **(S5)**, since 2017 has been extended into a software protection suite both by NAGRA-Kudelski and Thales.

The CTO of Software Monetization at Thales declared that:

“Our current Software Protection Suite is an essential building block securing a customer base of several thousand independent software vendors protecting billions of Euro of their revenue” **(S2)**

while the Senior Product Manager at Kudelski IoT stated:

“The Kudelski Obfuscation Product (KOP) is used for protecting Kudelski products in both Digital TV as IOT since 2012 and is since 2016 also commercialized for protecting third-party applications. The technology that has been developed in the ASPIRE project has partly been integrated into the KOP toolchain and is generating multiple millions of revenues on a yearly basis to the Kudelski Group” **(S1)**.

WeconStudio, since 2019, have been able to adapt the ASPIRE protections to make them work on IoT devices and, from then, all the security-sensitive parts have been protected with ASPIRE toolchain protections **(S3)**.

Impact on Police investigation practice in the UK and Overseas

Al-Nemrat helped to improve the digital forensics methods of the London Metropolitan Police. According to the force’s Head of Digital Forensics:

“The developed tool increased greatly the speed of investigations, by around 50% and reviewing images without the need to look at the actual source images. It also had a positive impact on the investigators’ mental health and wellbeing by reducing the amount of images viewed by circa 65%” **(S7)**.

In 2016, Al-Nemrat was invited to the EU Network and Information Security (ENISA) Workshop and the participants produced the security requirements report for Digital Service Providers (DSPs) **(S8)**, in which he contributed to the debate about mandatory incident notification for digital service providers.

In 2018, the Head of Information Assurance of the Portuguese National Security Cabinet reached out for assistance to shape their confidential strategy and policies for cyberwarfare that led to the adoption of new policy orientations **(S9)**.

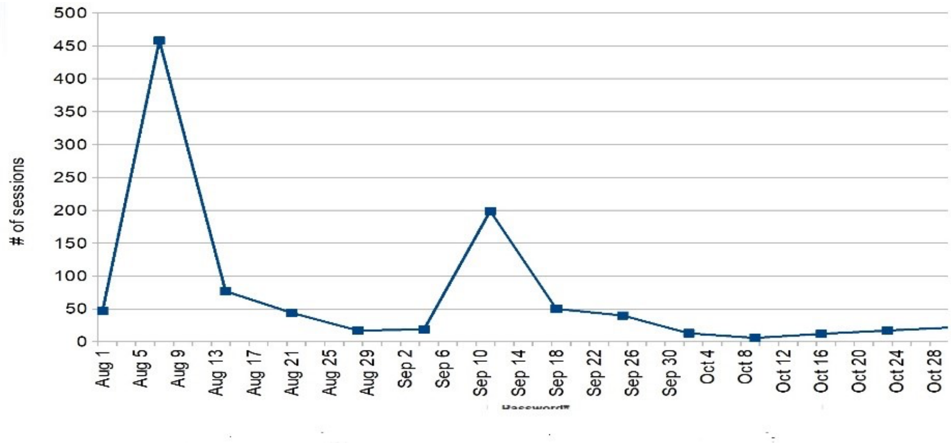
Al-Nemrat helped with cybercrime training police in Saudi Arabia and Algeria and his research on Incident Response Framework (IRF) **(R6)**, was the cornerstone of a comprehensive IRF for the UAE authorities **(S10)** that led in 2018 to the invitation by the UAE Ministry of Interior office to discuss and improve the cybercrime victimization policy and service pervision in UAE.

Wider impact and public awareness

All the software developed by UEL in ASPIRE is open-source and freely available **(S4)** as part of the ASPIRE toolchain **(S5).** A YouTube channel [F] was created with thirty demonstration videos of all the ASPIRE protections, reaching more than 10,000 views worldwide.

Falcarin created the International workshop on Software Protection (SPRO), co-chairing two editions and reaching more than 40 participants from industry in each edition.

The ASPIRE challenge in summer 2016 reached more than 900 users in three months, from more than 20 countries (Figure 1).



Croatia	225
United States	197
United Kingdom	95
Italy	85
Germany	45
France	42
Belgium	38
Netherlands	24
Switzerland	22
Madagascar	20
Israel	17
Australia	16
Japan	15
China	14
Canada	12
Norway	10
Russia	10
...	

Figure 1: Number of ASPIRE challenge sessions per week and users’ countries

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

S1. Letter from Senior Product Manager at Kudelski IoT

S2. Letters from Thales CTO of Software Monetization and Thales Software R&D Project Manager

S3. Letter from WeconStudio CTO, https://www.weconstudio.it/en/home-en/

S4. ASPIRE-UEL Code Renewability framework. On-line at https://github.com/UEL-aspire-fp7.

S5. ASPIRE Toolchain project open source software repository, https://github.com/aspire-fp7

S6. ASPIRE YouTube channel,
https://www.youtube.com/channel/UCntMGBjHr_oW5wEd5JgjD6g

S7. Letter from the former Director, Digital Forensics and Communication Unit – Metropolitan Police

S8. ENISA - Final report: Technical Guidelines for the implementation of minimum security measures for Digital Service Providers https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

S9. Letter from Portuguese National Security cabinet

S10. Abdelrahman Abdalla Humaid Al-Ali, Ameer Al-Nemrat: "Cyber Victimisation: UAE as a case study", in the Proceedings of the Cybersecurity and Cyberforensics Conference (CCC 2017). IEEE, pp. 19-24. 2017 https://ieeexplore.ieee.org/abstract/document/8252896