Institution: University of West London

Unit of Assessment: UOA 11 - Computer Science and Informatics

Title of case study: CyMonD: Commercial application of Cyber Monitoring and Defence for the Internet of Things

Period when the underpinning research was undertaken: 2012 to 2019

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:**
Junaid Arshad	Associate Professor in Cyber Security	Dec 2015 to Jan 2020
Kok Keong (Jonathan) Loo	Professor in Computing and Communication Engineering	Since June 2017
Christian Sauer	Senior Lecturer in Computer Science	Sept 2011 to Sept 2019
Thomas Roth-Berghofer	Professor of Artificial Intelligence	Sept 2011 to Jan 2017

Period when the claimed impact occurred: January 2018 to December 2020

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

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

Weaknesses in the cybersecurity of internet-connected consumer devices can undermine the privacy and safety of individual users, as well as risking large-scale cyber-attacks. Meeting these security challenges is a major issue for device manufacturers and service providers looking to exploit IoT-based technologies, especially for SMEs. Research undertaken at the University of West London, with support from Innovate UK / DCMS, led to the development of a novel tool - CyMonD - which offered protection against attacks. This development has led to beneficial collaborations with two SME's and commercialisation through a new University-led start-up in 2020.

2. Underpinning research (indicative maximum 500 words)

Assessments by Loo and Arshad had identified that although there were various IoT security solutions, they are all focussed on network traffic analysis rather than device-level security. A joint effort conducted by Loo and Arshad at UWL aimed at the research and development of cutting-edge solutions which enhance the security of Internet of Things (IoT) devices against the emergent cyber-physical attacks exploiting vulnerabilities within such devices. The team formulated a research program called Cyber Monitoring and Defence for IoT (CyMonD) which was funded by Innovate UK and DCMS under the Cyber Security Academic Start Up Accelerator programme (CyberASAP) between February 2018 and January 2019.

The innovation of CyMonD lies in its application of Linux mandatory access control mechanism and policy on IoT devices, along with cloud computing, secure distributed communication, machine learning and AI, to closely govern the operation of IoT devices against anomalous behaviour. CyMonD can protect against all the common traits of botnet attacks such as intrusive root access, device vulnerabilities, backdoor access, abnormal system processes and malware injection. It could also prevent zero-day attacks such as DDoS, ransomware and data breach through detection and defence at the device-level.

The collaboration drew on previous research advances in the AI domain in general at UWL by Sauer and Roth-Berghofer. Sauer and Roth-Berghofer had investigated challenges in knowledge extraction for case-based reasoning (CBR) systems [R1 and R2] (2012 to 2017 at UWL). The outcomes of this research helped the CyMonD team to formulate the knowledge extraction from data gathered by individual monitoring agents such as hosted on IoT devices.

Arshad led research to develop COLlaborative Intrusion DEtection for IoT (COLIDE) [R3 and R4] (2016-2019 at UWL) which investigated a collaborative approach to intrusion detection for IoT. COLIDE leveraged collaboration among resource-constrained IoT devices and edge routers to improve visibility of monitored activities for effective and timely detection of intruders without incurring significant performance costs. The research outcome informed the design of CyMonD in the distributed monitoring of IoT devices to achieve effective detection and prevention of malicious threats.

Loo has led the development of an innovative approach to improve the security of wireless sensor networks (WSN) and IoT. He was initially engaged in research focused at investigating protection for IoT devices against attacks targeting malicious URLs leading to development of an approach to detect malicious URLs using simulated expert (SE) and knowledge base system (KBS), 2017-2019 at UWL. [R5]

The proposed approach applied state-of-the-art machine learning methods to explore lexical features for more effective detection, avoiding the need for human expertise. The research outcome informed the design of CyMonD's anomaly intrusion detection based on machine learning and knowledge base system.

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

R1. Lara Quijano-Sanchez, Christian Sauer, Juan A. Recio-Garcia, and Belen Diaz-Agudo. 2017. Make it personal. Expert Syst. Appl. 76, C (June 2017), 36–48. https://doi.org/10.1016/j.eswa.2017.01.045

R2. Roth-Berghofer, Thomas, Recio Garcia, Juan Antonio, Sauer, Christian, Bach, Kerstin, Althoff, Klaus-Dieter, Diaz-Agudo, Belen and Gonzales Calero, Pedro A. (2012) Building case-based reasoning applications with myCBR and COLIBRI Studio. In: UKCBR 2012, 10 Dec 2012, Cambridge, UK.

R3. Arshad, Junaid, Azad, Muhammad Ajmal, Abdellatif, Mohammad Mahmoud, Rehman, Muhammad Habib Ur and Salah, Khaled (2018) COLIDE: A collaborative intrusion detection framework for internet of things. IET Networks, 8 (1). pp. 3-14. ISSN 2047-4954 https://doi.org/10.1049/iet-net.2018.5036

R4. Arshad, Junaid, Azad, Muhammad Ajmal, Abdeltaif, Muhammad Mahmoud and Salah, Khaled (2020) An intrusion detection framework for energy constrained IoT devices. Mechanical Systems and Signal Processing. Mechanical Systems and Signal Processing, Volume 136, 106436, https://doi.org/10.1016/j.ymssp.2019.106436.

R5. Anwar, S., Al-Obeidat, F., Tubaishat, A., Din, S., Ahmad, A., Khan, A.F., Jeo, G. and Loo, J. (2020) Countering malicious URLs in Internet-of-Thing (IoT) using a knowledge-based approach and simulated expert. IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4497-4504, https://doi.org/10.1109/JIOT.2019.2954919.

Grant: Innovate UK, Cyber Monitoring and Defence for IoT Devices (CyMonD) Lead Participant: The University of West London. Project Manager: J. Loo. Project reference numbers: 133568 (2018, £9,600), 133666 (2018, £16,000); 133738 (2018-2019, £100,000).

Quality statement: All of the references (except R2) have been published in peer-reviewed journals. R1 and R4 have been submitted as outputs by the University for REF 2021. In December 2020, R1 had 17 citations, R3 had 8, and R4 had 5 and R5 had 4.

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

Internet-connected consumer devices provide economic and social benefits but the weaknesses in the cybersecurity of these devices can undermine the privacy and safety of individual users, and also can be used for largescale cyber-attacks. Governments and regulators have paid increasing attention to these issues. In March 2018, the UK Government issued the *Secure by Design* report proposing that security is built into IoT products, rather than relying on consumers to take their own precautions.

Meeting these security challenges is a particular issue for device manufacturers and service providers looking to exploit IoT-based technologies, especially for SMEs. They need cost-effective tools to address cybersecurity requirements in order to innovate and bring new IoT-based products to market.

The development of CyMonD has contributed to this challenge, boosting innovation and entrepreneurship. This has taken place through two routes. First, by demonstrable collaborations between Arshad and Loo and innovative SMEs. Second, through the establishment of CyMonD Ltd as a spin-out company by UWL.

CyMonD development and spin-out

CyMonD was one of the 13 projects that won support to Minimum Viable Product (MVP) stage from the joint Department for Digital, Culture, Media and Sport and Innovate UK Year 2 *Cyber Security Academic Startups Accelerator Programme*, with three awards totalling £126,000 in 2018/19.

There was a successful demonstration of the MVP (functional software solution) at an Innovate UK public showcase event in January 2019. [S1] This contributed to attracting strong interest from investor firms that were looking to advance the technology with technical and financial support. In addition, CyMonD has attracted interest from existing vendors and across different components of the value chain that present opportunities for advancements through technological collaboration.

A UWL spin-out company – CyMonD Ltd – was formed in January 2020 to enable the full exploitation of the advances made by Arshad and Loo. [S2] As part of the due diligence relating to this spin-out, the University commissioned a review of the knowledge generated by Arshad and Loo and its commercial potential. The independent consultancy report in 2020 said that "CyMonD offers attractive, unique propositions to add another layer of cyber protection for IoT products at the device-level" and identified suitable routes to commercial exploitation and investment. [S3] Following the report the University entered negotiations with several commercial entities in relation to securing external investment into CyMonD Ltd to progress commercial exploitation. These negotiations began in 2020 and remained ongoing at the end of that year as their completion was hampered by the Covid-19 pandemic.

Collaborations for IoT innovation

Throughout the CyMonD project, Loo and Arshad took part in outreach organised by Innovate UK and the Knowledge Transfer Network, and collaborated with SMEs. Two of these SMEs have used this knowledge to improve their commercial products.

IMEDIAVAN Ltd, a London-based creative development team, developed a technological blueprint in 2019 for a smart-home solution on behalf of a European architecture firm which required this to build homes for the future equipped with IoT devices to automate household tasks. IMEDIAVAN were concerned about the security of these devices, and consulted with Arshad and Loo from June 2018 to January 2019 to make informed decisions about hardware, interactions between the devices and potential integration of CyMonD technology within their solution. The CEO of IMEDIAVAN has said: "These discussions helped us develop our solution which was delivered in May 2019 and took into account potential security threats for IoT devices. Furthermore, it has

helped us deliver not only the functional requirements expected by our clients but also to deliver these in a secure manner, which has indeed strengthened our offering for future customers". [S4]

Secure Technologies Ltd provide the technology and software that enable a network of 2000 electric vehicle charging pedestals and 2500 marina charging pedestals to supply electricity. These stations, which form the backbone of their infrastructure, were powered by a legacy microprocessor-based computing system. The company had been interested in adopting IoT technology but had taken the view that the security threats outweighed the benefits.

Secure Technologies' engagement with Arshad and Loo in 2019 alleviated the company's concerns, in particular through knowledge transfer regarding the design of connected IoT devices based on embedded Linux hardware and system design. As a result, the company put in a place a one-year plan from November 2019 to develop their own charging stations based on connected IoT devices, with a view to integrating CyMonD technology within their existing infrastructure as part of their products and services. A Director of Secure Technologies has written to confirm that they believe that the technology "..addresses one of the major concerns regarding IoT i.e. security hardening of IoT devices and we are keen to strengthen our collaboration with the team to transform our critical business operation into a smart and secure infrastructure". [S5]

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

S1. *Cyber Security Academic Startups Accelerator Programme*, Year 2 Demo Day, 17th Jan 2019.

S2. Companies House Filing: CYMOND Ltd, company number 12417897, 22nd Jan 2020.

S3. Confidential Report from New Prospect Business Solutions Limited, March 2020.

S4. Letter from CEO and Digital Director, IMEDIAVAN Ltd, 4th March 2020.

S5. Letter from Director, Secure Technologies Ltd, no date.