Institution: University of Gloucestershire

Unit of Assessment: UoA 12 General Engineering

Title of case study: Body Physiological Signal-Inspired Applications: Impact on Cyber Security

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:
Hassan Chizari	Associate Professor	2017 to present
Kamal Bechkoum	Professor	2016 to present
William Sayers	Senior Lecturer	2017 to present
Shujun Zhang	Professor	2012 to present

Period when the claimed impact occurred: 2017- 2020

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

1. Summary of the impact

The impact case study is based on the randomness extraction device from a collaboration between the University of Gloucestershire and Imperial College London. Hassan led three projects that developed a randomness extraction algorithm and methodology to generate strong cryptographic keys for Implantable Medical Devices (IMDs) from body physiological signals (four InnovateUK funds). The developed methodology includes a novel algorithm that provides secure communication between a medical implant and its gateway outside the body. Further, the project collaboration has identified a large set of authentication applications for wearable and other personal IoT devices, keyless autonomous vehicles and military and intelligence usages.

2. Underpinning research

Underpinning data analysis and cryptographic research for this project is based on three sets of journal outputs and completed projects. The first set of publications resulted from research in developing communication and routing algorithms among sensors (**R5** and **R6**), the second set of outputs are based on time series analysis methods in computing (**R3** and **R4**), and the final dataset was created using body physiological signals in securing medical implants (**R1** and **R2**).

From the underpinning research we extract randomness from body physiological signals, where our experiments and comparative studies with quantum random number generators show very high quality (entropy) extraction. The extracted randomness was used to generate a cryptographic key in two steps. In the first step, both IMD inside the body and its gateway outside the body will undertake the processing at the same time in order to land on the same keys, without the need to have a key exchange process (**R1**). Since the analogue body physiological signal cannot be read similarly inside and outside the body, it is inevitable that IMD and its gateway could not end up having the same key. In the second step of the developed algorithm, based on the idea of Fuzzy Vault a message which is encrypted with symmetric cryptography is decrypted with a close replica key. The combined processes are responsible for generating the randomness, forming the key, and processing the key agreement protocol based on the idea of similar key cryptography. The result is a secure authentication protocol without a key exchange process, creating opportunities for exploitation (**R2**).

Another perspective to this research was to work on timeseries analysis methods, in order to provide better understanding on how to measure noise when receiving data from sensors (such as body physiological sensors). This research had an empirical study on state-of-the-art mathematical methods for noise filtering focusing on three main areas: extracting precise and reliable data from noisy sensors, detecting anomalies where one or a specific group of sensors are providing highly noisy data, and finally data outliers for one or a group of sensors (**R3**). Alongside with this review study, we developed a decentralised noise detection and correction method called Local Outlier Detection Algorithm (LODA). Developed algorithm is designed to be implemented in sensors with very limited resources especially computational power and memory which are the two key facilities in most of outlier and noise reduction algorithms (**R4**).

Sensors' communication protocol and routing is another dimension of underpinning research. In order to develop such protocol a comprehensive review of the state-of-the-art work in routing protocols for underwater sensors have been undertaken. A taxonomy analysis on the literature has been completed with key challenges on how to provide a reliable and void aware routing identified (**R5**). Further, we developed a location-free reliable and energy efficient routing algorithm for underwater sensor networks. This is a lightweight information acquisition algorithm which provides much better performance in packet receive ratio while maintaining low energy usage in sensors (**R6**).

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

Research Outputs:

R1 Chizari, Hassan, Emil Lupu, and Paula Thomas. "Randomness of physiological signals in generation cryptographic key for secure communication between implantable medical devices inside the body and the outside world." Living in the Internet of Things: Cybersecurity of the IoT (2018): 27-6.

R2 Chizari, Hassan, and Emil C. Lupu. "Extracting randomness from the trend of IPI for cryptographic operators in implantable medical devices." IEEE Transactions on Dependable and Secure Computing (2019).

R3 Safaei, Mahmood; Asadi, Shahla; Driss, Maha; Boulila, Wadii; Alsaeedi, Abdullah; Chizari, Hassan; Abdullah, Rusli; Safaei, Mitra. 2020. "A Systematic Literature Review on Outlier Detection in Wireless Sensor Networks." Symmetry 12, no. 3: 328.

R4 Safaei, Mahmood, Abul Samad Ismail, Hassan Chizari, Maha Driss, Wadii Boulila, Shahla Asadi, and Mitra Safaei. "Standalone noise and anomaly detection in wireless sensor networks: A novel time-series and adaptive Bayesian-network-based approach." Software: Practice and Experience 50, no. 4 (2020): 428-446.

R5 Khasawneh, Ahmad, Muhammad Shafie Bin Abd Latiff, Omprakash Kaiwartya, and Hassan Chizari. "Next forwarding node selection in underwater wireless sensor networks (UWSNs): Techniques and challenges." Information 8, no. 1 (2017): 3.

R6 Khasawneh, Ahmad, Muhammad Shafie Bin Abd Latiff, Omprakash Kaiwartya, and Hassan Chizari. "A reliable energy-efficient pressure-based routing protocol for underwater wireless sensor network." Wireless Networks 24, no. 6 (2018): 2061-2075.

4. Details of the impact

(a) Cyber security of medical implants

Descriptions: As part of CyberASAP InnovateUK project more than 8,000 vulnerabilities have been revealed by testing only four manufacturers' peacemaker in June 2017 by Whitesmoke. The main reasons for those vulnerabilities were not using encryption methods for communication or using static key communication. Although some solutions have been proposed in research literature recently, the market still lacks a comprehensive methodology to provide such security for medical implants. The technology that we have developed addressed this challenge and provides a novel comprehensive secure protocol for these devices. The idea is that both medical implant and gateway outside the body read a specific body physiological signal (IPI or QRS) and then generate the communication key after that. This key will be secure, without key exchange process and it is also temporary. It means that after the communication session expired, the key acquisition process needs to be repeated again. Such ability provides very light, yet very powerful communication security for medical implants. This project has been reviewed and mentored by internationally recognised Crossword Cybersecurity plc (**C1**) (https://www.crosswordcybersecurity.com)
who have accelerated commercialisation of the technology. Further, Boston Scientific (https://www.bostonscientific.com/en-US/Home.html) and Food and Drug Administration (FDA) (https://www.fda.gov/medical-devices) in USA have showed interest in the developed solution with regard to this technology and the urgency of adapting the solution to current medical implants vulnerabilities.

(b) True randomness generation:

Description: As part of CyberASAP InnovateUK project (BioGenerate phase one and two) the core of cybersecurity is cryptography and the heart of cryptography is randomness. Without having a high-quality randomness generator, it is not possible to achieve high level cyber security. Recent reports showed that even some of Quantum Random Number Generators (QRNG) are not providing the quality of randomness they promised. In algorithm that we developed, physiological signals (specially EEG) show a very high quality (entropy) and generation rate which can compete with QRNGs. These two qualities (entropy and speed) are not usually coming together in randomness generation. This is an amazing opportunity for those applications which need to have true randomness, to use device independent high-quality randomness from the human user of the service. We have signed an NDA with CryptaLabs (**C2**) (https://www.cryptalabs.com) who confirm the validity and potential where human presence is important. Additionally, software cybersecurity company Secure Technologies Ltd (**C3**) (https://secectltd.co.uk) confirm the applicability of the technology for internet service providers.

(c) Other applications:

Description: Also, as part of CyberASAP InnovateUK project (BioGenerate phase one and two) upon developing the product, this innovation has been identified to have the potential of exploiting a wide range of markets and to compete with expensive solutions such as quantum random number generators as presented by CYLON (**C4**) (https://cylonlab.com). As a result of the development of this innovation, we are working on potential commercial exploitation to start from 2022 in a global market worth 26 Billion Dollar (the Active Medical Implant Devices) and 506 Million Dollar (Random Number Generation). In this regard, both Crossword Cyber Security (**C1**) and CYLON (**C4**) have been collaborating with the University of Gloucestershire regarding commercial feasibility study for a business start-up in 2022. Targeted applications are for authentication protocols and secure communication wherever human presence in a cyber setting is crucial. For instance, one of the areas which has been identified by Crossword Cyber Security (**C1**) is keyless autonomous cars. In this application, temporary secure keys are generated between driver and the car, which the driver is using to get access to the car later one. Every time the driver touches the steering wheel for more than 30 seconds (to read body physiological signal specifically IPI), a new pair of keys are being generated for the car. To use the key the driver's body physiological signal is needed and having access to the car's key itself, will not let the intruder to have access to the car. Another identified application is authentication and secure communication between devices of emergency services such as firefighters or police. In such scenario, all the devices of a policeman authenticate themselves with himself not by using a static key, but a dynamic key generated from the heartbeat of the policeman at the time of authentication.

5. Sources to corroborate the impact

C1 - Testimonial, Jake Holloway, Chief Product Officer, Crossword Cybersecurity.

C2 - Testimonial, Joe HQ Luong, CEO Crypta Labs Ltd.

C3 - Testimonial, Jeeta Aulak, Director Secure Technologies Ltd.

C4 - Testimonial, Joanna Wlazlak, Director of Product CyLonCyLon Ltd.