Cyber Security Academic Startups Accelerator Programme Year 2
Phase 2: Market Validation of Value Proposition
1st June 2018

Project Titles/Summaries	Universities
Low Power & High Speed True Random Number Generator *Securing communications in IoT applications*	Liverpool John Moores
Secure communications with implantable medical devices using body signals	Gloucestershire & Imperial College London
ExpertSecure *Learning and automating security expert decision making when analysing and configuring security controls*	Huddersfield
CyMonD *A software platform to protect IoT/smart devices against botnet exploits*	West London
CityDefend *A searchable encryption enterprise solution giving users full control over their cloud data*	City London
TAME *A semi-automated web-based threat assessment platform*	Hertfordshire
ZER0 Trust Security *A granular-level perimeter enforcement platform based on entity attributes*	Manchester Metropolitan
ACTI - Adaptive Cyber Threat Intelligence *Informing and optimizing CISO cyber security decision-making*	De Montfort
Security Monitoring and Administration Residential Toolkit *Protecting home users from digital trauma*	Oxford
Cydon- An Intelligent and Decentralised Data Management Platform *Optimised E-discovery and secure data sharing*	Wolverhampton
Verifiable E-Voting *End-to-end verifiable self-enforcing electronic voting without use of tallying authorities*	Newcastle & York
HuaHana *Designing and visualising security into software*	Bournemouth
CofDrop *A highly private and anonymous desktop/mobile messaging app*	City London
Raven *Find, classify, and analyse extremist multimedia*	City London
“Smoke Detector” for IoT Security *Detecting IoT attacks by monitoring physical behaviour*	Cardiff
Authentication in Voice-controlled Platforms *Automatic authentication for secure transactions from home, on the & Lloyds Bank move and in public places using voice-controlled platforms*	London Metropolitan & Lloyds Bank
PriDevOps Toolkit *Automating the integration of privacy-by-design principles throughout DevOps software development processes*	University of Brighton

Low Power & High Speed True Random Number Generator

Securing communications in IoT applications

Liverpool John Moores University

The Internet of Things (IoT) is a fast-growing market where data encryption is required during the communication phase. Modern encryption algorithms rely on random numbers for cryptographic operations in almost all the security standards. Conventional random number generation based on complex mathematics is under threat due to fast growing computing capabilities. A new technique for random number generation is urgently required to enhance the security of IoT devices during real-time protection. We have developed such a solution which enhances the quantum effect in widely-used CMOS technology and from which we harvest true randomness with simple digital circuits. The high-quality random number can be generated with low cost and low power consumption, making it an ideal solution for future IoT appliances.

Team

Our team includes the experts in hardware, software and IP management. Dr Zhigang Ji has been working on the development of emerging technologies and their applications for over 10 years. As well as his renowned reputation in the academic community, Dr. Ji also has rich industrial experience and has been on advisory boards in many companies. Dr Bo Zhou is the expert in cybersecurity. He served as director within the largest state-owned software company in China before joining LJMU. Dr Zhou's experience in both academia and industry makes him a strong candidate to commercially develop this project and ensure the market needs are addressed while providing the required technology innovation. Dr Alison Hardy is the LJMU IP & Commercialisation Manager. She will provide assistance and guidance with the project's commercialisation and exploitation plans, including the development of licencing models and spinout company formation whilst ensuring full appropriate protection of IP.

Secure communications with implantable medical devices using body signals

Lead University: University of Gloucestershire
Partner University: Imperial College of London

The vulnerabilities of Implantable Medical Devices (IMDs) have been surfaced in many reports specially in year 2017 where hundreds of thousands of patients and/or IMD manufacturer were affected by those. The main causes of these problems are the weak authentication and weak secure communication between IMD inside the body and the gateway outside the body. By nature, an IMD has very limited resources and using general secure computing solutions on it is not feasible. The idea of using body physiological signals to generate a random number which then will be used to generate a key for communication has been introduced for a few years. However, till now, no empirical solution has been developed to generate strong random numbers from body physiological signals. What we have developed is a strong random number extractor which generate communication secret key and use it with the concept of similar key cryptography to provide a high level of security for IMDs communication.

Team

Dr. Hassan Chizari (University of Gloucestershire): Experienced in developing IoT devices and received several innovation awards for developing "Early flood detection radio sensor network", "Air quality monitoring sensor network" and "Flash flood detection in urban areas". Currently, he is working with Prof. Emil Lupu in developing a secure communication platform for IMDs using the physiological signals as the source of randomness.

Prof. Emil Lupu (Imperial College London): Emil Lupu is Professor of Computer Systems in the Department of Computing at Imperial College London. At Imperial, he leads the Academic Centre of Excellence in Cyber Security Research, the Resilient Information Systems Security Group and serves as Associate Director with the Institute for Security Science and Technology. Emil is also Deputy Director of the PETRAS IoT Security Research Hub – Cybersecurity of the Internet of Things.

Prof. Shujun Zhang (University of Gloucestershire): Shujun Zhang has rich experiences of transferring research and development results into the industrial products. His latest work is research, design and development of bio-inspired systems using human physiological signals.

ExpertSecure

Learning and automating security expert decision making when analysing and configuring security controls

University of Huddersfield

Monitoring the vast array of information sources within IT systems to identify potential security problems and perform mitigation activity is challenging and requires significant expertise. Many businesses are facing challenge with recruiting and maintaining cyber-security expertise and this deficit is resulting in many being left unable to adequately monitor their systems. ExpertSecure facilitates less skilled users in acquiring cyber-security specific knowledge, tailored to their system and enabling them to perform in-depth monitoring and mitigation activities. There are many solutions to assist with automating security analysis and configuration activities; however, their knowledge-base is manually constructed by human experts. This is time-consuming, costly, and can limit the usefulness of the solution if insufficient knowledge is available. ExpertSecure is capable of autonomously extracting and automation security analysis and configuration activity from monitoring security activity without any additional human resources.

Team

Dr Parkinson currently holds post as Senior Lecturer at the University of Huddersfield. Through his research he is developing niche expertise within the cybersecurity area of Security Information and Event Management (SIEM). Their research is driven to address to global cybersecurity skills shortage by equipping non-specialist users with software tools to perform expert-equivalent security analysis and configuration activities. For example, they have developed a software application for analysing file system permissions, which has had over 50k installations.

Dr Parkinson has recently co-edited a book entitled Guide to Vulnerability Analysis for Computer Networks and Systems - An Artificial Intelligence Approach, acquired £0.7 million in research income, and currently has a team of 5 full-time PhD researchers. Dr Parkinson holds post as a cybersecurity advisor on the West Yorkshire Police Independent Cyber Security Group. He also sit on the advisory panel for the Yorkshire Cyber Security Cluster and the Digital Catapult’s cyber security programmes.

CyMonD

A software platform to protect IoT/smart devices against botnet exploits

University of West London

Security for IoT devices is critical today and beyond. A typical IoT device is an internet facing embedded computer, once deployed it forms part of a critical infrastructure e.g. smart environment., and they often left unattended. There are overwhelming concerns in security and privacy by the users, amid the serious unconsented/unnoticed exploitation of IoT devices e.g. the global widespread cyber-attacks by Mirai botnet in October 2016. These attacks exemplified the vulnerabilities of IoT devices to security threats as well as providing a glimpse into potential consequences of successful attacks including attempts to hijack critical national and international infrastructures. Our project, CyMonD sets out to meet the technological gaps, by developing an effective security capability to defence and deter adversaries to the IoT devices and its operation environment. More specifically, CyMonD develops a runtime, monitoring and defence mechanism at device-level which is able to protect against botnets (an automated hack to exploit the vulnerabilities and backdoors) and other known and unknown threats.

Team

The project team comprised of Professor Jonathan Loo and Dr Junaid Arshad. Jonathan has 15 years of research experience and expertise in computing, communications, electronics, IoT technology, and cybersecurity. He has completed 7 funded research projects (EU, UK and overseas), 18 PhD completions, and contributed more than 240 peer-reviewed publications. On the other hand, Junaid has strong experience in investigating and addressing novel security issues for emerging paradigms. He has gained in-depth knowledge of Linux-based systems through developing programs interfacing Linux kernel and working with processes and application programs via system call representations. The team is active in the research surrounding malware analysis on android platform focusing dynamic malicious traits and behaviour, and is exploring new paradigm in detecting and preventing malware of zero-day attack. The team envisages to leverage these experiences and expertise to achieve the objectives of the CyMonD project.

CityDefend

A searchable encryption enterprise solution giving users full control over their cloud data

City, University of London

According to Forresters, the global cloud market is showing a compound annual growth rate (CAGR) of 22% [1]. However, 75% of enterprises have highlighted security concerns related to the cloud storage. In addition, 60% of enterprises have highlighted data protection concerns [2]. These concerns prevent people from outsourcing their private and confidential data to the cloud. We provide Searchable Encryption-as-a-Service (SEaaS) to the client's so that they can securely outsource their data to any 3rd party Cloud. Unlike our competitors, our solution reduces the storage overhead and the network latency, whereas it is scalable across cross-cloud platforms. This in effect gives people full control of their personal data along with trust onto the Cloud. Our market share is US $1.5M.

Team

Muttukrishnan Rajarajan (project lead and founder) is a Professor of Security Engineering at the City, University of London, UK and has an experience working in the area of information security for well over 18 years. He obtained his Ph.D. in Information Engineering from City, University of London in 2001. His research expertise are in the areas of cloud security, privacy of things and internet of things security. He is currently leading cyber security related projects funded through EPSRC, H2020, UKIERI, Royal Academy of Engineering, UK industries and the Innovate UK.

Shahzaib Tahir (co-founder) is a Research Assistant at the City, University of London. He received his B.E. degree in Software Engineering and MS degree in Information Security in 2013 and 2015 respectively. He is actively involved in research on Cloud security, cryptography and privacy preserving techniques including searchable encryption. During his research studies he has worked with British Telecommunications UK and Intelligent Voice on research projects related to Searchable Encryption. He has worked from initial research idea to full scale implementation on commercial systems.

References

[1] L. Columbus, https://www.forbes.com/sites/louiscolumbus/2017/11/07/forresters-10-cloud-computing-predictions-for-2018/

[2] UK Cloud Adoption & Trends For 2016 https://www.cloudindustryforum.org

TAME

A semi-automated web-based threat assessment platform

University of Hertfordshire

We will develop a Cyber-Threat Assessment platform called TAME (Threat Assessment Model for Information Environments). The platform will deliver a threat modelling service to organisations in a landscape in which the scale of cyber threats continues to evolve and increase. Following extensive research in phase 1, it was decided that the project would target the legal sector. According to a PCW survey, 59% of law firms in the UK are planning on using big data and predictive analytics technologies for business support. The top two identified priorities for these UK law firms over the next 12 months is to improve the use of technology and to standardise and centralise processes regarding security assessments. TAME will support the delivery of these sector-wide strategic objectives. There are numerous firms in the cyber market place that state they deliver threat assessment solutions, focusing on a technology-based analysis, requiring the use of expensive external resources. TAME is innovative in that it allows assessors within the business, who possess knowledge of their information environment, to undertake internal assessments and provide easily digestible threat modelling information based on business assets and processes to key decision makers. TAME will benefit businesses by providing them with an efficient, portable and scalable solution for self-assessing their cyber threats and structuring the regulatory defensive information operations they should be undertaking. TAME will reduce IT expenditure, effectively removing the need for expensive external cyber threat assessors and therefore directly enhancing the company's profitability.

Team

Dr Stilianos Vidalis is the academic lead. Dr Vidalis' involvement in Information Operations began in 2001. Since then, he has accrued extensive cyber security experience and a PhD in threat assessment. He has participated in and led high profile, high value projects for large international organisations and Governments. He has implemented access controls in secure environments. He has collected and analysed threat information for European financial institutions. He has trained the British Armed Forces (all services) for a number of years in the collection and analysis of cyber intelligence. He is working with covert and non-covert Law Enforcement Units. Within the spinout, he will operate as the CTO and Director of Operations.

Mr. Jeeta Aulak is a retired Detective Inspector. He is experienced in intelligence and threat assessment through work in Counter Terrorism, the NCA and working alongside CEOP. During his time at the NCA he co-authored the National Threat Assessment from Organised Crime to the UK borders. He has an MSc in financial crime investigation. Mr. Aulak will be the CEO and also undertake the Finance and Business Development Director roles in the company.

Mr. Anthony Edwards, a former Managing Partner of a law firm, and now a Non-Executive Director of a law firm. He has launched a number of companies in the past. Mr. Edwards will undertake the role of the business advisor.

Prof. Andy Jones has a defence background. He is an expert in digital forensics and in threats to information systems. He is the Director of the Cyber Security Centre at the University of Hertfordshire. Prof Jones will undertake the role of product development advisor.

ZER0 Trust Security

A granular-level perimeter enforcement platform based on entity attributes

Manchester Metropolitan University

ZER0 Trust brings a new and first rigorously verified theory of zero trust to provision a vendor-free Platform as a Service (PaaS) that utilizes existing and new technologies and governance processes to leverage granular perimeter and micro-segmentation enforcement based on users attributes to determine whether to trust a user, machine or application seeking access to a particular part of the enterprise network from anywhere. It aims to develop a secure, reliable, scalable, and high-performing platform to provide streamlined and secure access to enterprise resources. This modular platform will integrate existing and new threat protection, encryption, activity monitoring, access control, malware protection and other security management functions to provide an end-to-end zero trust security solution. This product will offer a single unified platform to protect live data, reducing complexity and operational costs with a ‘single pane of glass’ style management of all threats. It will leverage automation to re-program every device within minutes of a new attack being detected.

Team

Dr Mohammad Hammoudeh has skills in threat analysis information and network security management, penetration testing, cyber and insider investigations, and breach assessments and incident response.

Jawad Mohsin has skills in in cybersecurity and threat analysis, software development, distributed computer system design, static security analysis, security system design and implementation.

Dr Bamidele Adebisi has skills in advanced distributed systems, specifically the Internet of Things, analysis and design. He has a strong track record in successful application of customer-focused approach to the full system development lifecycle.

Dr Umar Raza has expertise in system security engineering. He leads the collaboration and communication with stakeholders to develop a range of mitigating control strategies into the zero trust.

Dr Paul Hooper has overall responsibility for business development activities in the Faculty of Science and Engineering, with dedicated resources to support academics in decisions around IP protection and commercialisation routes with external partners. He sits on the University's IP review group and commercialisation committee, whose remit is to support, track and commercialise IP. He has worked closely with internal and external parties in supporting commercialisation activities.

ACTI - Adaptive Cyber Threat Intelligence

Informing and optimizing CISO cyber security decision-making

De Montfort University

Our business called ACTI will develop adaptive cyber threat intelligence (CTI) solution to help security critical businesses to optimise their security investment and resource utilisation. The unique feature is that we will visualise security investment in real time and especially we will target on both IT systems and Industrial Control Systems. Specifically, this innovation is a proactive decision support system that incorporates CTI, allowing decision makers to trade off real time security investment and operations against current, emerging threats. This innovation will tailor the CTI to the organisation's most relevant emerging threats and recommend selected and tailored security solutions to help prioritise security investments. The innovation will apply novel mathematical models to analyse, quantify and prioritise relevant threats, and present investment trade-offs to decision makers.

By making the security investment transparent, this innovation will benefit both security critical businesses, especially those dealing with critical national infrastructure (CNI), and cyber liability insurance companies. This innovation will bring a transformative change of the relationships between the two parties. We will continuously seek advice on requirements and exploitation from the Industrial Advisory Group (Airbus, BT, Deloitte and Rolls-Royce) of the Cyber Technology Institute in De Montfort University (DMU) during the project.

Team

Dr. Ying He (Academic Lead) is a Senior Lecturer in DMU. Her research interests are Security Decision Making, Risk Analysis and Threat Intelligence (leading DMU HEIF project DPPI).

Dr. Iryna Yevseyeva is a Senior Lecturer in DMU. Her research interests are Multi-Criteria Optimisation and Decision-Making in the security context (Airbus project GaCS).

Prof. Helge Janicke is the Head of School of Computer Science and Informatics at DMU. His interests include SCADA and Industrial Control System (ICS) Security. He established DMU's Airbus Group Centre of Excellence in SCADA Cyber Security.

Prof. Eerke Boiten is the director of the Cyber Technology Institute at DMU. His research interests include Privacy and Data Protection and Legal Aspects of cyber security (GDPR, NIS), Threat Intelligence (EU H2020 project NeCS), and Ransomware (leading EPSRC project EMPHASIS).

DMU Commercialisation Team (Dr. Paul Burrows and Ms Nadia Omar) will support a two-pathway commercialisation through De Montfort Expertise Limited (DMEL).

Industrial Advisory Group (IAG): We will continuously seek advice from our Industrial Advisory Group (Airbus, BT, Deloitte and Rolls-Royce) during the project.

Security Monitoring and Administration Residential Toolkit

Protecting home users from digital trauma

University of Oxford

We want to help home users to protect themselves, their friends, and their families from serious and growing digital threats.

Our research shows that home users look for unitary and personalised solutions, and seek to build a trust relationship with those supporting their IT needs: security is an intrinsic part of their wider digital well-being.

Our solution is to provide a wellness approach to digital security in the home, combining user-centered technology and services to help protect home users against current and future threats and also empowering them to achieve the digital well-being they seek. Initially, we target employee wellness companies, providing added value to the employee assistance market that currently does not address this need.

Our core product is a user-centered Security Monitoring and Administration Residential Toolkit (SMART) for managing home digital security. This device and its software will enable the home user to manage the security of home networks, and perform other security actions in a simple and user-friendly manner: increasing the security capability of home users. To complement the SMART device we will offer additional support services, providing advice, information resources, and incident management support that is confidential, accessible, appropriate and personalised.

Team

Ivan Flechais is an Associate Professor in the Department of Computer Science at Oxford and has over 15 years' expertise in the area of secure and usable systems design. He has published extensively in the areas of secure systems design, usable security & privacy, and home data security and privacy, and also has significant experience in leading and delivering academic research projects funded by the UK and EU.

Norbert Nthala is a final year Doctoral student under the supervision of Prof. Flechais. His research has explored the issues of home data security decision-making and his work to date has uncovered detailed information regarding informal and social support activities in home data security. Prior to starting his DPhil, Norbert worked in network engineering and management consulting.

Cydon- An Intelligent and Decentralised Data Management Platform

Optimised E-discovery and secure data sharing

University of Wolverhampton

This project aims to design and develop a secure, scalable GDPR-compliant solution that is capable of data storage and processing with evidentially acceptable levels of detail while sending alerts in real time to the officer responsible for critical digital evidence using blockchain (BC) technology. Given both the nature of the records held and transmitted as well as their total size, BC will be utilised as a vital component to ensure that the records are treated in such a way that their integrity, authenticity, and confidentiality are always assured. The proposed solution is promised to minimise execution times in remote monitoring and data collection processes, log rotation, storage, and processing of the communication networks currently utilised by police forces. The main idea is that after several blocks, it should be computationally infeasible to change a block containing transactions. The complexity of the proof of work scales dynamically with the combined computation in the network. This is, indeed, the first time that such a technology is used in that context, which by itself provides a unique testbed for the academic team to produce innovative solution(s) that are immediately applicable to support the forensic activities of policing services.

Team

Dr Gregory Epiphaniou has worked as a cyber security consultant and trainer for QA Ltd., with high engagement with several industry partners in information security domains. Gregory has also been a leading trainer and developer for bespoke cyber security programmes, with a dedicated, strong team of experts and trainers in several technical domains in both offensive and defensive security. He has also contributed to numerous public events and seminars in cyber security, course development and effective training for both private and governmental organizations. His current position is as reader in cybersecurity at the University of Wolverhampton, and has been contracted in several commercial and research projects. Prof Prashant Pillai is working as a directors of the Wolverhampton Cyber Research Institute at the the University o Wolverhampton. Prof Prashant has over 15 years of research experience and specialised in the area of communication protocols and cyber security. He received his BSc in electronics and did his PhD in the field of network security from University of Brandford, UK. With educational background in electronics and IT security and an avid interest in AI, Prof Prashant has a passion of researching complex issues in safety critical systems like smart grid, autonomous cars, aeronautical systems and robotics.

Verifiable E-Voting

End-to-end verifiable self-enforcing electronic voting without use of tallying authorities

Newcastle University (in partner with University of York)

This project aims to assess the commercial viability of “self-enforcing e-voting” (SEEV), a new generation of e-voting systems that are end-to-end (E2E) verifiable without tallying authorities. E2E verifiable voting systems are widely regarded as the best available solution to protect an e-voting system from fraud and tampering, let it be for polling station voting or for Internet voting. However, existing E2E verifiable voting systems generally rely on a set of tallying authorities (TAs) who are supposedly trustworthy individuals with computing and cryptographic expertise to perform complex decryption and tallying operations. Finding and managing such TAs in practice has proved to be particularly difficult. Our solution, developed under the support of an ERC starting grant and an ERC proof of concept grant, overcomes this major problem by applying novel cryptographic techniques to achieve E2E verifiability but without requiring any tallying authorities. In other words, the voting system is "self-enforcing". The removal of TAs significantly simplifies the election management and makes an E2E verifiable voting system much more practical than before. We have implemented fully working SEEV prototypes for both polling station voting and Internet voting, and conducted user trials with positive feedback. Newcastle University has filed patent applications to protect the IPR of the SEEV invention. With this startup program, we aim to capitalize on the pending IPR and to explore the commercial opportunities of our research output.

Team

This is a collaboration project between Newcastle University and University of York.

The Newcastle University team includes Dr Feng Hao (Reader in Security Engineering), Dr Ehsan Toreini (Research Associate) and Mr Graeme Young (Business Development Manager).The University of York team includes Dr Siamak Shahandashti (Lecturer in Security). Dr Hao is the PI of the ERC Starting Grant on “self-enforcing electronic voting”. He received his PhD in Computer Science from University of Cambridge. He co-invented DRE-i and DRE-ip, two end-to-end verifiable e-voting systems without tallying authorities. Previously, he invented J-PAKE, which has been adopted by the Thread Group as an industry standard for secure communication in Internet of Things (IoT) and built into real-world IoT products including Google Nest, ARM mbed, NXP IoT gateway. Dr Ehsan received his PhD in Computer Science from Newcastle University. He specializes in anti-counterfeiting and security in web technologies. Mr Young is a business development manager in Newcastle University's enterprise team, responsible for academic commercialization, IPR, finance and business liaison. Dr Shahandashti received his PhD in computer science from University of Wollongong. He specializes in cryptography. Previously, he invented broadcast encryption schemes, which have been used in millions of pay-TV devices built by Thales. He co-invented DRE-ip.

HuaHana

Designing and visualising security into software

Bournemouth University

We expect our software to be secure. Software is useless if people cannot or will not use it, but software is built to deliver value not security which makes achieving usable security a struggle for designers. To break this impasse, we present HuaHana: the first commercial platform for designing demonstrably usable and secure software. HuaHana supports the workflows of security and usability designers by organising their design assets, and finds security problems early and quickly by validating and visualising even the most basic of software designs.

Team

Our team has delivered world-class research in the design of usable and secure software for over 10 years, and we wrote the first textbook on the design of usable and secure software. However, unlike most academic startups, our team also has a track record in delivering world-class software too. We have built software that ensures boilers are safely installed in homes around the UK, facilitated trading at one of the world's largest energy derivates markets, and controlled operations for spacecraft sent to Mars and Venus. For the last 8 years, we have also maintained CAIRIS: the open-source technology platform upon which HuaHana is based.

CofDrop

A highly private and anonymous desktop/mobile messaging app

City, University of London

Freedom of speech is a legal right but practically people can be afraid to speak out due to fear of surveillance, repercussions, censorship, or repressive governments. It is well known that privacy in electronic communications is elusive. CofDrop is a mobile and desktop application to send messages, or any file, privately and anonymously. CofDrop enables anyone to share confidential information with journalists, police, social services, and other organisations, without fear of surveillance or tracking.

Team

Tom Chen is a Professor in Cyber Security at City, University of London. He has 8 years of industrial R&D experience and 20 years of academic experience in the US and UK. His research has been supported by US National Science Foundation, UK research councils, and several companies.

Dr Jorge Blasco is a Lecturer in the Information Security Group at Royal Holloway, University of London. He contributes his expertise in Android programming and information security.

Dr. Carol Daniel and Powlami Ghosh are members of City's Research & Enterprise office.

Raven

Find, classify, and analyse extremist multimedia

City, University of London

Our vision is to develop automated and intelligent technologies to locate and identify malicious contents online. Our main technology is Raven, an intelligent web crawling system for finding, identifying, and analysing extremist videos using advanced machine learning techniques. Extremists are taking advantage of social platforms for propaganda, recruitment, and radicalisation. Raven helps Internet companies and law enforcement to find and take down extremist multimedia. Raven automates the analysis of video contents for counterterrorism.

Team

Tom Chen is a Professor in Cyber Security at City, University of London. He has 8 years of industrial R&D experience and 20 years of academic experience in the US and UK. His research has been supported by US National Science Foundation, UK research councils, and several companies.

Dr Jorge Blasco is a Lecturer in the Information Security Group at Royal Holloway, University of London. He contributes his expertise in machine learning and information security.

Dr Daniel Wolff is a former postdoc research assistant at City. He contributes his expertise in machine learning and Python programming.

Dr. Carol Daniel and Fay Kassibawi are members of City's Research & Enterprise office.

Consultants to the project:

Professor Julio Hernandez-Castro at University of Kent contributes his expertise in cyber security.

Counter Terrorism Internet Referral Unit (CTIRU) in the London Metropolitan Police.

“Smoke Detector” for IoT Security

Detecting IoT attacks by monitoring physical behaviour

Cardiff University

IoT means Internet of Things – a combination of the virtual and the physical worlds. And attacks on the IoT affect both. So why limit your IoT security monitoring to what you can see by capturing network traffic? Our solution is like a smoke detector – passive, non-intrusive, and focussed on external symptoms. We do not care about network or device internals, we observe visible physical behaviour. We use a range of sensors to monitor status LEDs, motion patterns, sounds, temperatures – anything that the devices may do. Using edge computing and machine-learning, we check for anomalous and malicious behaviour and then raise an alert. We can alert the user directly or feed alerts into existing threat-detection systems.

Team

Dr Philipp Reinecke is a Lecturer in the School of Computer Science and Informatics at Cardiff University. Prior to joining the university, he worked in Hewlett Packard's Security and Manageability Lab in Bristol. His skills are in systems modelling, machine-learning, and systems development, particularly in the area of cybersecurity.

Prof. Omer Rana heads the Complex Systems group at the School of Computer Science and Informatics at Cardiff University. He has extensive experience of industry engagement through a number of InnovateUK projects, including direct consultancy. He supports the InnovateUK funded "IoT Accelerator for Wales" as an academic partner. Prior to joining Cardiff University, he worked as a software developer with London-based Marshall Bio. Tech Limited.

Dr Parisa Eslambolchilar's expertise is in user-centred design and the challenges involved in developing systems with the user's requirements in mind.

Dr Padraig Corcoran provides expertise in machine-learning and data-science for the further technical development of the solution.

Matthew Turner is the Software Academy Manager & Knowledge Transfer Officer. His expertise and contribution are in business development.

Authentication in Voice-controlled Platforms

Automatic authentication for secure transactions from home, on the & Lloyds Bank move and in public places using voice-controlled platforms

Leading University: London Metropolitan University
Partner Organisation: Lloyds Banking Group

We expect our software to be secure. Software is useless if people cannot or will not use it, but software is built to deliver value not security which makes achieving usable security a struggle for designers. To break this impasse, we present HuaHana: the first commercial platform for designing demonstrably usable and secure software. HuaHana supports the workflows of security and usability designers by organising their design assets, and finds security problems early and quickly by validating and visualising even the most basic of software designs.

Project & Team

Our technology allows you to use voice-controlled platforms such as Alexa, Siri and Google Assistant to execute financial transactions - from buying things online to checking your bank balance - in an easy and secure way.

As voice-based platforms become more widely used the old methods of passwords, fingerprint scanners and face recognition won’t work. Our solution solves this problem.

To deliver this project we have brought together 3 researchers and 5 postgraduates from the Cyber Security Research Centre at London Metropolitan University (LMU), alongside experts in IPR, knowledge transfer and commercialisation from the Accelerator at LMU.

Through our partnership with Lloyds Bank we will bring this technology to market and provide voice authentication security solutions to the financial sector, insurance companies and internet service providers, allowing them to unlock secure voice-controlled access to millions of users.

The need for this technology is particularly acute for the millions of people in the UK with visual impairment and severe dyslexia who currently struggle to use text-based systems. And as the trend towards voice-based platforms increases our solution will become increasing mainstream.

PriDevOps Toolkit

Automating the integration of privacy-by-design principles throughout DevOps software development processes

University of Brighton

We are passionate about data privacy. Our core technology ensures privacy takes centre-stage throughout the software development process, supporting DevOps teams to integrate privacy-by-design principles into the development of software products. Incorporated into the Privacy-by-Design toolkit, our technology enables companies to comply with privacy regulations such as GDPR by automating the process of developing privacy-aware software products without adding any delays to the software systems development process. The Privacy-by-Design toolkit facilitates data privacy at two levels, firstly by enabling organisational privacy policies and regulations to be translated into simple privacy requirements and secondly, by generating automated recommendations for DevOps teams to deploy solutions to fulfil those privacy requirements.

Team

PriDevOps' technology is the result of an extensive body of research led by Professor Haris Mouratidis, Director of the Centre for Secure, Intelligent and Usable Systems (CSIUS) and Professor of Software Systems Engineering at the University of Brighton. Haris has published more than 150 papers at the intersection of software engineering and security/privacy engineering. His work has been applied through pilots, industrial research & knowledge exchange projects to a range of application domains including public administration, critical infrastructures, cloud computing, health-care, telecommunications, banking, and e-commerce.

Dr Michalis Pavlidis is Senior Lecturer in Information Systems Security at the University of Brighton, and has published more than 15 papers relating to engineering privacy-aware and trustworthy information systems. Michalis has applied his research with industry and the public sector, and is creator of the JTrust approach for trust management, developed in collaboration with BT.

The academic team is supported by the University of Brighton Enterprise team, led by Dr Shona Campbell, and Jim Byford, a Digital Innovator, who has vast and varied experience in strategy development for tech start-ups.