



Academic  
Startup  
Accelerator  
Programme

## Overview of Projects selected for Market Validation stage of 2020/21 cohort\*

University of:

### **Bournemouth - Authentibility Pass**

*Application for people with disabilities to communicate authentication/accessibility requirements to organisations.*

Authentibility Pass will enable people with disabilities to efficiently communicate their authentication and accessibility requirements, which will be stored in secure organisation databases. This eliminates the need for customers to repeat their requirements. Employees will be more aware of suitable methods to support customers, resulting in higher customer satisfaction.

### **Bristol - A Tamper Guard and Intrusion Monitor using Zenneck Electromagnetic Surface-waves**

*Making surfaces that identify, verify and protect themselves.*

SurfaceRF, a University of Bristol spin-out, manufactures enclosures that detect when they have been touched on their surface for critical infrastructure and digital networks – a sector worth \$31 Bn in 2017 and predicted to grow to \$58 Bn by 2023. We are seeking development partners and seed funding.

### **Cardiff - CyCIS**

*Advanced Cyber Threat Detection & Incident Impact Tool for Infrastructure Resilience*

64% sophisticated attacks with 30% undetected threats on critical energy OT infrastructure can easily trigger block-outs to businesses. Unlike other tools, CyCIS is a unique data capture automation tool specially designed for infrastructure resilience through remote monitoring that not only detects acute threats but also exclusively evaluate their impact and predicts future risks.

### **Edinburgh Napier - Memcrypt**

*Memcrypt protects and recovers confidential data from ransomware attacks.*

Ransomware costs businesses around \$169 billion across the world. Our novel techniques detect and extract cryptographic keys from computing devices. This enables the protection and recovery of confidential data from ransomware attacks. This Edinburgh Napier University spin-up is looking for investors to develop a product to combat ransomware.

### **Essex - SenseiChain**

*Redefining the future of Blockchains through secure real-time data analytics*

SenseiChain is a highly secure pioneering solution that enables the monitoring and analytics of encrypted Blockchain transactions in real-time. This disruptive technology pioneers the analysis of sensitive information within and beyond organisational boundaries with complete trust, security and control, thus enabling revolutionary Blockchain capabilities.

### **Imperial College - Perfect Privacy Preservation as a Service**

*Unrivalled value from sensitive data silos with mathematically guaranteed privacy*

Our platform removes the trade-off between data utility and privacy. It combines privacy-preserving techniques in mathematics and encryption to enable analytics and machine learning without exposing identifying information. This unlocks new possibilities for businesses across highly regulated industries to safely create value from sensitive data assets with privacy by design.

#### **Imperial College - WhatML: Watermarking Machine Learning Models**

*WhatML protects the value and the intellectual property of machine learning models.*

Machine learning models are very valuable assets that require significant investments. However, existing forms of monetising these models cannot be used without an adequate way of protecting them. To solve this limitation, WhatML protects the intellectual property of machine learning models through watermarking, enabling verification of their ownership and provenance.

#### **Kent - #ID Security of IoT**

*Secure Device Identity to power the future of the Internet of Things*

#ID is a highly novel technology for deriving secure, unique identifying encryption keys from the measurable properties of digital systems, enabling minimal cost provision of digital identity for low cost IoT devices in security sensitive verticals associated with major growth trajectories.

#### **Lancaster – Developer Security Essentials**

*A non-profit helping consultants make the 400,000 UK developers better at security*

We offer consultants Security Essentials, an open-source (and subscription based) package of workshops, that inspires developers to incorporate security and motivates further consultancy work. Proven in a dozen organisations, the package is regularly updated and can be repeated with new teams and projects.

#### **Leeds – Developing a Quantum Inspired Key Distribution**

*Enhanced Automatic Fraud Detection and Quantum Secure Transactional Platform to protect everyone.*

B2C

We are building the most secure payment card security system ever for the financial sector by combining automatic fraud detection with quantum secure communications. Cards will now detect when they have been used fraudulently by themselves, and our post-quantum algorithms guarantee future-proof security for any transaction or communication.

#### **Leeds - Artificial Behaviour-Based Authentication for IoT (ABBA-IoT)**

*Data tampering detection system for automotive sensors*

ABBA-IoT is a data tampering detection system that monitors the network of sensors in a vehicle to detect anomalies in real-time. The unique algorithm behind ABBA-IoT offers the adaptability of machine learning approaches and the precision of key-based authentication techniques. ABBA-IoT provides trust in the data received from sensors.

#### **Liverpool – Flexible Querying of Encrypted Graph Databases**

*Query your graph data while keeping it encrypted with full user's control.*

Data is protected when encrypted. To use your data you need to decrypt it, and potentially to reveal it to a spyware. Not anymore. Our research led to the prototype tool which allows to query graph data while keeping it protected at all times. We have rights to commercialize and looking for investors to support further development.

#### **London South Bank – Victory – Secure VNF Service Management in 5G using Blockchain**

*'Victory' provides a reliable and secure service management for Edge-Cloud resources.*

VICTORY offers an Edge-Cloud orchestration framework that applies Deep Learning for reliability-prediction of the Edge-servers and secures service migration using blockchain. It provides a platform-agnostic solution to extend the capability of a virtualized infrastructure. The framework provides an API driven model that enables external applications to enhance its functionalities.

### **Middlesex - Threat Hunting System Based on Linux Security Hardening and Mandatory Access Control Policies**

*A Security assessment tool for Linux systems based on the MITRE Framework*

IoT cyberattacks could cost UK economy £1bn/an, around 80% of these systems run Linux OS. Building on our research in the area of intrusion detections and years of experience in security testing, we are looking for £60,000 to fund our deployment of an intelligent threat hunting and security assessment tool for Linux systems

### **Nottingham – AI-DRIVES – AI-Driven Secured Connected and Autonomous Vehicles**

*Connected vehicles will reduce 13% road accidents: But are they safe?*

By 2026, all new cars in the UK will be connected. However, the on-board transceivers are not fit for secured communications yet, vulnerable to cyber risks. At Nottingham our AI technology provides an easy-to-adapt solution for Tier 1 automotive transceiver suppliers to enter the market of \$7BN by 2024.

### **Plymouth – MaCRA (Software Tooling for Maritime Cyber Risk Assessment)**

*Dynamic, Multi-Dimensional Risk Assessment for Holistic Appraisal of Maritime Specific Operations*

MaCRA brings together vulnerability analysis, cyber and cyber-physical, and an understanding of the maritime sector, and all its niches, under one platform to help large global organisations with growingly complex IT and OT infrastructure assess and mitigate maritime cyber risks.

### **Southampton – CyberHelper**

*CyberHelper is an innovative tool that efficiently runs your cyberattacks' investigations.*

CyberHelper is a tool for the analyses of threats and evidence left after a cyberattack. It combines innovative techniques from network security, malware analysis, AI, and social sciences. CyberHelper increases the efficiency of the investigation by providing the analyst with AI-driven insights and guidance.

### **Strathclyde – Lupovis: A Wolf in Sheep's Clothing**

*Lupovis provides AI-driven deception solutions to detect threats and automate incident response.*

Lupovis provides an active deception-based defence system for early threat detection, analysis and automated response to insider threats, ransomwares and stolen credentials. Advance machine learning manipulates attackers to reveal themselves leading them away from crown jewels, protecting both complex OT and IT infrastructures and accelerate incident response.

### **UCL**

*Service Resilience Capability Assessment Tool (SR-CAT)*

UCL's SR-CAT provides TEN achievable steps towards cyber-resilience of smart city services. We create an assurance methodology mapped to NCSC, NIST and ENISA guidelines for business' and public authorities working on smart-city initiatives such as smart roads, cars and homes by providing an assessment tool to achieve cyber-resilience. We are currently helping London councils design cyber-resilient procurement requirements for smart street infrastructure.

### **Wolverhampton – CyberMIND**

*An AI-based platform helping Cybersecurity professionals to detect, predict, and manage stress*

Cyber Professionals protect our organisations and critical infrastructures. But 48% are suffering from mental health issues due to high stress. So how secure are we? CyberMIND is an intelligent platform designed to detect, predict and manage stress. Helping you improve team performance and staff wellbeing and reduce cyber-risk.

\*These projects will undergo a further selection process by independent assessors to determine which go forward to Stage 2 of CyberASAP 2020/21. The teams selected will receive funding to develop their Proof of Concept. This will be demonstrated in February at the culmination of this year's programme.

If you would like to know more about any of these projects please contact [Emma Fadlon](#) or [Robin Kennedy](#).

[CyberASAP](#) is funded by the UK Government Department of Digital, Culture, Media and Sport through Innovate UK and KTN.