Cyber Security Academic Startup Accelerator Programme

Year 2 Demo Day

17th January 2019

CYBER ASAP

CyberASAP Stakeholders

Department for
Digital, Culture
Media & Sport

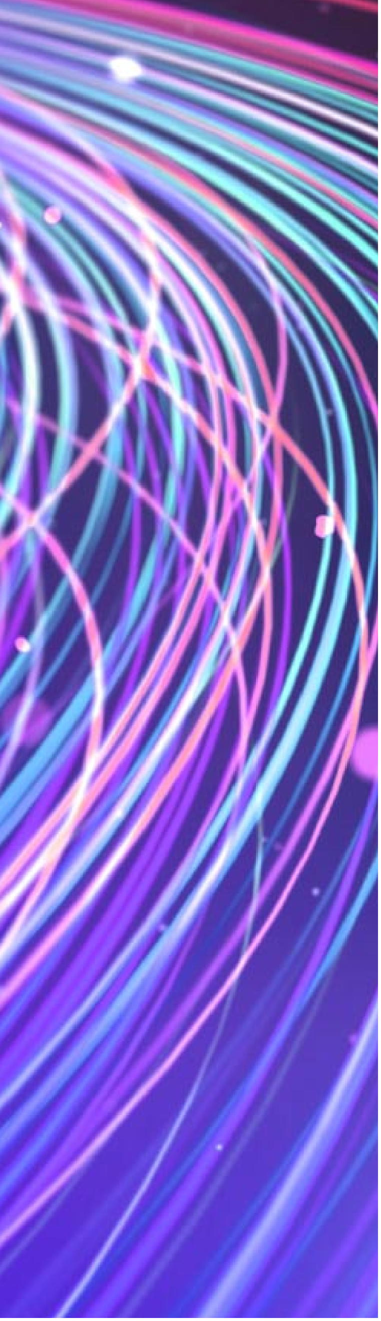
Innovate UK

Knowledge Transfer Network

CyberExchange
Connect Engage Collaborate

Booklet design by Starbit.

FSC
www.fsc.org
MIX
Paper from
responsible sources
FSC™ C005094



Introduction

The Department for Digital, Culture, Media and Sport (DCMS) is leading the Government's work to develop the world's best digital economy. We want the UK to be the best place to start and grow a digital business, and the most secure place in the world to live and do business online.

The 2016 National Cyber Security Strategy (NCSS) set out the Government's vision for the next five years: the UK is secure and resilient to cyber threats, prosperous and confident in the digital world. Our three broad strands of activity are to defend our cyberspace, to deter our adversaries and to develop our capabilities.

The UK cannot become the world's leading digital nation and be the best place to do business online unless organisations within the UK are secure and resilient. A crucial part of this is promoting the UK's cyber security sector, ensuring government, industry and academia work together to support a thriving ecosystem of successful, innovative companies.

This work supports DCMS's overall mission, which is **to ensure every organisation in the UK is cyber secure and resilient to support a prosperous digital nation.**

Agenda

Welcome: Dr. Emma Fadlon, Knowledge Transfer Network

Keynote: Margot James MP, Minister of State for DCMS

Pitches from Cyber Security Academic Startups

Tabletop Showcase/Demonstrations, Networking & Drinks

Pitch Running Order

Raven
City, University of London
Find, classify, and analyse online extremist videos

Social media platforms are facing regulatory pressure from UK and EU governments to take down extremist online contents quickly. Raven is intelligent software to find, classify, and analyse extremist videos. It combines advanced machine learning, image object recognition, and crawling. Raven has been developed in partnership with extremism experts, trained using thousands of videos, and tested by law enforcement.

Raven offers considerable savings in time and staff resources to law enforcement and social media platforms. Raven can automatically classify videos or extract important objects from videos to aid human moderators. In the future, Raven will be expanded to other problem domains involving illicit videos and images.

Notes

RAVEN SCIENCE

Contacts

Prof. Tom Chen
Lead Academic
tom.chen.1@city.ac.uk
+44 (0)2070 408926

Powlami Ghosh
IP and Commercialisation
powlami.ghosh@city.ac.uk
+44 (0)2070 400277

ravenscience.com

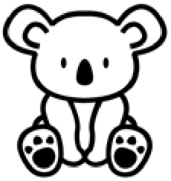
HuaHana
Bournemouth University

HuaHana. Enabling agile teams to create digital products and services with security and privacy designed in

Innovative apps need great user experience (UX). However, with the arrival of GDPR, Product owners and UX designers are grappling with how to design great products without security getting in the way. Product design needs timely security input, but nothing in the market facilitates UX and security design collaboration without sacrificing the agility designers need.

HuaHana meets this need by helping UX and security designers find security problems early by analysing and visualising product design data. By supporting agile design workflows and providing GDPR compliance checks earlier than any other product on the market, HuaHana is the first product that integrates both UX research and design into agile design lifecycles.

Notes



Contacts

Dr Shamal Faily
+44 (0)7808 475784
sfaily@bournemouth.ac.uk
@ShamalFaily
linkedin.com/in/shamalfaily

huahana.com | twitter.com/HuaHanaPlatform

CITYDEFEND

Protecting your online data

CityDefend
City, University of London
CityDefend-A searchable encryption enterprise solution for the Cloud

CityDefend, a searchable encryption enterprise solution giving users full control over their Cloud data.

CityDefend is a pioneering technology that allows clients to outsource large amounts of encrypted data onto the Cloud while being able to search. CityDefend provides military-grade security that can resist distinguishability attacks using its state-of-the-art search query generation mechanism. Our solution eliminates the need of a centralised data-structure, hence, reduces the network latency, storage overhead and provides scalability across cross-cloud platforms; thus enhancing the privacy of the system. CityDefend in effect gives people full control over their data on the Cloud resulting in trust on the Cloud services. CityDefend could have a profound impact on verticals including healthcare, telecommunications, financial, public services, law enforcement and many other sectors.

Notes

CITYDEFEND

Protecting your online data

Contacts

Prof. Muttukrishnan Rajarajan
+44 (0)207 040 4073
raj.rajarajan@citydefend.com

Dr Shahzaib Tahir
+44 (0)739 907 8631
shahzaib.tahir@citydefend.com

Powlami Ghosh
IP and Commercialisation Consultant
+44 (0)2070 400277
powlami.ghosh@city.ac.uk

citydefend.com | twitter.com/CityDefend | linkedin.com/company/citydefend

Security Monitoring and Administration Residential Toolkit (SMART)

University of Oxford

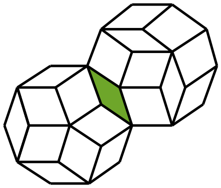
Empowering home users for digital wellness and protection

We are a spinout from the University of Oxford that helps home users achieve confidence, safety, and wellbeing for digital work and leisure at home through an employee assistance programme.

Our business helps home from attackers harming the home (e.g. identity theft, ransomware, cyberbullying, and employees of sensitive companies targeted at home), and homes becoming instrumental in attacking others (e.g. Distributed Denial of Service Attacks from compromised home devices on critical infrastructure, compromised remote working computers, or malware infection vectors).

We are developing an application and a device to help secure the home environment from current and foreseeable threats. We provide added value to the employee assistance market that currently does not offer a wellness solution to home digital security. Our business also offers companies a light-touch and flexible way to help remote workers – permanent or freelance – protect themselves and their work.

Notes



Contacts

Ivan Flechais
Associate Professor - Computer Science
ivan.flechais@cs.ox.ac.uk

Catherine Spence
Senior Licensing & Ventures Manager
catherine.spence@innovation.ox.ac.uk

Norbert Nthala
Doctoral Student
norbert.nthala@cs.ox.ac.uk

digiwell.web.ox.ac.uk/smart

CyMonD

Intelligent IoT Insight

CyMonD
University of West London
Smart security for smart infrastructures

IoT devices can be deployed to build smart infrastructure e.g. smart cities, industrial IoT etc., which bring benefits to the operators and users. However, IoT device is the weakest link in the IoT ecosystem.

We developed CyMonD solution, to address the big challenge in managing IoT security at large-scale, especially against the rising cyber-physical attacks, such as botnet and physical tempering of IoT devices. CyMonD is a device-level solution that offers, i) real-time monitoring and defence with minimal human invention, ii) AI-powered access control policy management against cyber-physical hacks, and iii) an enhance device security, yet scalable to large-scale infrastructure.

CyMonD USP addresses a number of areas in the IoT value chain, such as access control policy, active monitoring and proactive device protection that are currently not the mainstream. In its operation, CyMonD monitors IoT devices' system behaviour, and generate access control policy adaptively powered by AI, and apply to the devices. Through this operation, CyMonD is able to protect IoT devices proactively, and able to safe-guard smart infrastructure.

CyMonD breaks new ground in IoT security. To the best of our knowledge, CyMonD is the first solution to apply access control policy to govern how IoT devices operate. In fact, CyMonD is complementary to some existing solutions, and it can be integrated to form a comprehensive IoT security.

Notes

CyMonD

Intelligent IoT Insight

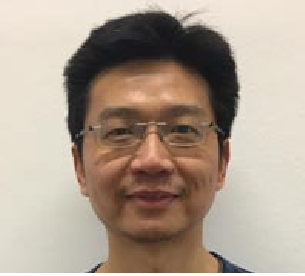
Contacts

Professor Jonathan Loo
jonathan.loo@uwl.ac.uk
+44 (0)208 231 2921

Dr Junaid Arshad
junaid.arshad@uwl.ac.uk
+44 (0)208 231 2351

SEEV

SELF-ENFORCING E-VOTING



SEEV
University of Warwick (in collaboration with Newcastle University & University of York)
Verifiable electronic voting for real-world

SEEV offers secure e-voting systems for real-world elections, with the initial focus on online shareholder voting. The security of an e-voting system is critical for assuring the integrity of the election result, thus assuring the integrity of democracy.

Our patented self-enforcing e-voting (SEEV) technology enables voters to verify the tallying integrity of the entire voting process, in the meanwhile preserving the voter privacy, without requiring any trusted tallying authorities. While focusing on online shareholder voting initially, we envisage our e-voting products will cover all election scenarios in the real world, let them be conducted over the Internet or onsite at polling stations.

Notes

SEEV
SELF-ENFORCING E-VOTING

Contacts

Feng Hao
feng.hao@warwick.ac.uk
+44 (0)7515 866 183

seevtechnologies.com

CrypTier
University of Hertfordshire
TAME – threat assessment model for information environments

Traditional approaches to cyber-security do not work for targeted one-off attacks. They only automate the detect and deny stages in the responder's kill chain.

Our technology can be used to automate the disrupt, degrade and deceive stages, effectively overcoming the inevitability of a compromise.

Our USP is partly based on the modelling modelling techniques we use for understanding the vulnerability interrelationships of business-critical assets (tangible and intangible). This understanding is then coupled with situational awareness data for analysing the threat agent motivation, capability and attack opportunity.

Our technology can identify the path of least resistance and the shortest path to an asset.

Notes

CrypTier

Contacts

Dr. Stilianos Vidalis
s.vidalis@herts.ac.uk
Cyber Security Centre
University of Hertfordshire
College Lane, Hatfield, AL10 9AB, UK

@CrypTierLtd | linkedin.com/in/CrypTierLtd

Event Horizon Security

Event Horizon
University of Huddersfield
Autonomous identification and exploitation of security expertise from Security Information and Event Management data sources

Monitoring the vast array of information sources within IT systems to identify potential security problems and perform mitigation activity is challenging and requires skilled experts. Many businesses are facing challenge with recruiting and maintaining cyber-security expertise and this deficit is resulting in many being left unable to adequately secure their systems.

Research undertaken at the University of Huddersfield has resulted in the development of an intelligent technique capable of the autonomous extraction of analysis and configuration activities from monitoring security activity without any additional human resources. The technique – Event Horizon – then uses this knowledge to facilitate less skilled users, enabling them to perform in-depth monitoring and mitigation activities.

There are many solutions available 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.

Notes

Event Horizon Security

Contacts

Dr Simon Parkinson
Lead Academic
s.parkinson@hud.ac.uk
+44 (0)1484 472525
@DrSParkinson

Saad Khan
Researcher
s.khan@hud.ac.uk
@ySo0oSeri0us

ehsecurity.co.uk

air ID

airID
London Metropolitan University
Easy use of voice controlled devices with guaranteed security

The AirID team specialises in developing complex solutions for enabling voice controlled devices to be used for perfroming transactions which require guaranteed security. These solutions utilize the recent hardware, software and communication technologies which shape today's industry - the Cloud, Internet-of-Things and Voice Communications.

This project aims at developing a technical solution which enables the use of voice-controlled devices for executing financial transactions in an easy and secure way. We are surrounded by clever devices everywhere – at home, on the way while walking, driving or traveling, and in public places. Some of them even understand us by just talking, like Amazon Alexa, and they are becoming more wide spread by day. But the society needs more from technology to improve quality of life. Today it is possible to connect most of these devices to the Internet easily. Imagine how exciting it would be to be able to ask them to check your balance, or to order buying your ticket by just talking ... Unfortunately, at the moment it is not possible due to the low level of security of voice-controlled devices. The technology must provide the opportunity to use services everywhere in an easy way with guaranteed security and this is exactly what the project devivers.

Our solution is complex because it requires combining of several of the hottest technologies in Cyber Security – security of the Internet of Things, security on the Cloud and security of the Signal Processing.

Notes

air ID

Contacts

Vassil Vassilev
Project Leader
v.vassilev@londonmet.ac.uk
+44 (0)7762794997
linkedin.com/in/vvassilev

Karim Ouazzane
Director Research and Enterprise
k.ouazzane@londonmet.ac.uk
+44 (0)7717680820
linkedin.com/in/professor-karim-ouazzane-59904b28

londonmet.ac.uk/research/centres

NanoSec
Liverpool John Moores University
Low-power and high-speed True Random Number Generator (TRNG)

Low-power and high-speed True Random Number Generator (TRNG)

A unique security module for the use in RFID tags for security-sensitive healthcare applications

Over 4% of the incidents in NHS are due to patient misidentification, risking patient safety, satisfaction, and hospital revenue. RFID provides an effective solution to reduce misidentification and improve operational efficiency. However, due to the limited resources, true random number generator, as a key element for security, cannot be implemented in RFID tags.

We developed a hardware-based true random number generator (TRNG) tailored for RFID applications, tackling five critical challenges simultaneously: security, power consumption, reliability, chip area and cost. It has pasted the rigours NIST random test making it readily to be implemented in future RFID technology.

Notes

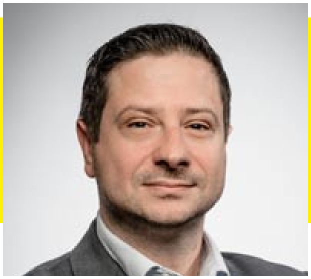
NANO SECURITY

Contacts

Dr Zhigang Ji
Lead Academic
z.ji@ljmu.ac.uk
+44 (0)151 2312505

Dr Alison Hardy
IP & Commercialisation Manager
a.hardy@ljmu.ac.uk
+44 (0)151 904 6371

PRIVACYLABS



Privacy Laboratories
University of Brighton
Preventing data breaches by taking privacy centre-stage throughout the software development process

Consumers have increasingly high expectations with respect to the privacy of their data with awareness rising daily thanks to media coverage. And now, GDPR requires organisations to comply with high standards of data privacy, or face hefty fines.

Privacy Laboratories offers a novel software toolkit that prevents costly and reputationally damaging privacy breaches, by taking privacy centre-stage throughout the software development process. Optimised for DevOps, our toolkit automates the process of incorporating privacy in the software lifecycle process, and integrates privacy culture in the organisation. It is adaptable so it can be integrated with your organisation's existing software development tools and processes, with consultancy and training ensuring ease of adoption.

The Privacy-by-Design toolkit provides multiple views to inform different stakeholders on privacy issues and violations, enabling organisations to evidence compliance with privacy regulatory requirements (such as GDPR) by providing privacy-by-design reporting capabilities.

Notes

PRIVACYLABS

Contacts

Professor Haris Mouratidis
Professor of Software Systems Engineering
h.mouratidis@brighton.ac.uk
linkedin.com/in/harismouratidis

Dr Shona Campbell
Assistant Director, Enterprise
s.e.campbell@brighton.ac.uk
linkedin.com/in/shona-campbell

privacylabs.co.uk

ACTIVE
De Montfort University
Adaptive Cyber Threat Intelligence for Security Investment Optimisation

Due to GDPR, all organisation have to invest into security. There are lots of security defense solutions available in the market, but how much to invest and how to distribute investment and into which resources?

Our company, ACTIVE, provides an adaptive cyber threat intelligence solution to help decision makers/CISO to optimise security investment and resource utilisation. The unique feature is that we visualise security investment in real time and provide a reporting dashboard, allowing CISO to produce reports to justify security cost.

By making the security investment transparent, this product will benefit both security critical businesses, especially those dealing with critical national infrastructure (CNI), and cyber liability insurance companies.

Notes

ACTIVE

Contacts

Ying He
ying.he@dmu.ac.uk
+44 (0)116 257 7614
linkedin.com/in/ying-he-91245954

Iryna Yevseyeva
iryna@dmu.ac.uk
+44 (0)116 250 7540
linkedin.com/in/irynayevseyeva

active.nuvelle.co.uk

CYDON
SHARE DATA CONFIDENTLY

Cydon
University of Wolverhampton
Cydon: An intelligent decentralised data management platform

Traditional centralised data storage and processing solutions and those that utilise Clouds, manifest some limitations with regards to overall operational cost and the availability, usability and security of the data. One of the biggest problems with these existing solutions is the difficulty of keeping track of who has had access to the data and how the data may have changed over its lifetime while providing a secure and easy-to-use mechanism to share the data between different users.

Cydon is a dedicated data management platform based on a patented algorithm that utilises smart ledgers for electronically regulating data sharing across organisational boundaries and supply chains. The technology enables quick and immutable search, regulates the creation and processing of data requests across different organisational units and provide authorised and faster access to secure distributed data. It dramatically reduces time to access data, avoids single points of failure by securely distributing data across untrusted nodes and provides immutable transaction logs with an "always-on" chain of custody.

Notes

CYDON
SHARE DATA CONFIDENTLY

Contacts

Prof Prashant Pillai
CEO
p.pillai@cydon.co.uk
linkedin.com/in/prashant-pillai-prof

Dr Gregory Epiphaniou
CTO
g.epiphaniou@cydon.co.uk
linkedin.com/in/dr-gepiphaniou

Prof Andrew Pollard
TTO – University IP Manager
a.pollard@wlv.ac.uk

cydon.co.uk | linkedin.com/company/cydon

Commercialising UK Academic Ideas

CyberASAP Programme Directors

Robin Kennedy
Cyber Security
robin.kennedy@ktn-uk.org
+44 7870 899956

Dr Emma Fadlon
Access to Funding & Finance
emma.fadlon@ktn-uk.org
+44 7964 551643

Knowledge Transfer Network	ktn-uk.org	@KTNUK
CyberASAP	cyberasap.co.uk	@CyberASAP