Cyber Security Academic Startup Accelerator Programme

Year 3 Demo Day
13th February 2020

CYBER
ASAP

Background to CyberASAP

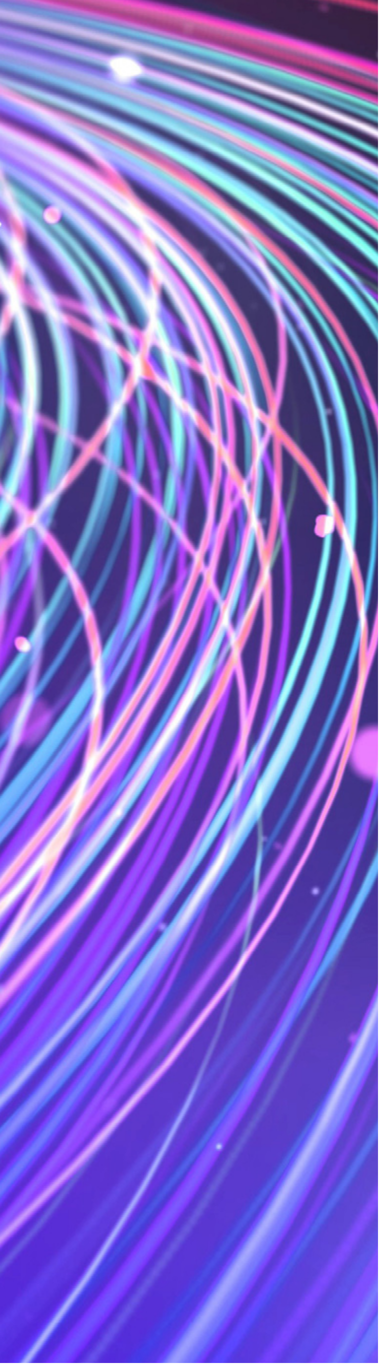
The Department for Digital, Culture, Media and Sport (DCMS) is leading the Government's work to develop the world's best digital economy. DCMS wants the UK to be the best place to start and grow a digital business, and the most secure place in the world to live and do business online. The National Cyber Security Strategy (NCSS) set out the Government's vision to 2021: the UK is secure and resilient to cyber threats, prosperous and confident in the digital world. The three broad strands of activity are to defend our cyberspace, to deter our adversaries and to develop our capabilities. 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.

DCMS funds CyberASAP which is delivered through Innovate UK and the Knowledge Transfer Network.

Department for
Digital, Culture
Media & Sport

UKRI Innovate UK

Knowledge Transfer Network



Programme Overview

The only pre-seed accelerator programme in the Cyber Security ecosystem, the Cyber Security Academic Start-up Accelerator Programme (CyberASAP) exists to help commercialise academic ideas in the cyber security space.

About to enter its fourth year, CyberASAP provides a comprehensive range of support to develop academics' entrepreneurial skills and translate their research into products and services. Through a varied, year-long programme of expert workshops, training, briefings and bootcamps CyberASAP helps teams at every stage along the complex journey from lab to market.

The programme operates over three stages, supported by external assessments and with input from experts within the KTN as well as its wider network of industry specialists.

1A **Developing a Value Proposition**
1B **Market Validation of the Value Proposition**
2 **Development of a Proof of Concept**

Graduates of the programme, 20 teams so far, have been encouraged to progress their projects, going on to achieve a range of successes including: acquisition by technology firms; receiving seed funding; joining other accelerator programmes; securing government grants; partnering with commercial enterprises.

In helping accelerate the roll out of great cyber security ideas from universities, CyberASAP supports the ecosystem and DCMS's aims to develop and sustain a security sector that meets the national security demands; and in so doing creates a dynamic interface between government, cyber security academics and the business and investment community so vital to the health and development of this sector.

Agenda

Welcome: Dr. Emma Fadlon, Knowledge Transfer Network

Pitches from Cyber Security Academic Startups

Keynote: Matt Warman MP, Minister for Digital and Broadband, DCMS

Tabletop Showcase/Demonstrations, Networking & Drinks

Pitch Running Order

PriSAT | University of Glasgow
Automated Assurance of Privacy-by-Design in Software Systems Pages 4-5

The Privacy Tool | Bournemouth University
Software that enables DPO roles to rapidly improve confidence in organisational Privacy Risk status Pages 6-7

INSURE | De Montfort University
Portable Wireless Intrusion Prevention Systems for Smartphones and Tablets Pages 8-9

GuardKeeper | Coventry University
Advanced authentication and secure connections in hostile environments Pages 10-11

OnlynShield | University of Wolverhampton
Intelligent safeguarding software shielding children from harmful online communications Pages 12-13

Prinesec | Royal Holloway
Creating causality chains to empower predictive threat detection Pages 14-15

PhishAR | University of Oxford
Phish-proofing user authentication by harnessing the power of AI and AR Pages 16-17

BioGenerate | University of Gloucestershire and Imperial College London
Securing device to device communication Pages 18-19

BLEMAP | Royal Holloway
Bluetooth security and vulnerability insight [in a blink] Pages 20-21

Draconia | Bournemouth University
Cost-effective, bolt-on service for advanced threat detection Pages 22-23

Verifiable Credentials | University of Kent
Replacing all credentials, including passwords, with W3C standardised, cryptographically-secured, electronic credentials Pages 24-25

TAPCHA | Bournemouth University
Online fraud prevention, CAPTCHA reinvented for everyone & every device Pages 26-27

SPYDERISK | University of Southampton
Automated risk assessment for enterprise IT compliance Pages 28-29

PriSAT

Privacy Engineering for Software Designers

University of Glasgow

PriSAT
University of Glasgow
Automated Assurance of Privacy-by-Design in Software Systems

Privacy-by-Design has always been part of data protection law, and a key change with regulations such as GDPR and CCPA is that it is now a legal requirement. The objective of Privacy-by-Design is to help companies achieve regulatory compliance by embedding a set of foundational privacy principles into the design specification of technologies. But the challenge for business is the lack of any approach to tangibly demonstrate that they have rigorously followed Privacy-by-Design to certify regulatory compliance. PriSAT is a Privacy-by-Design technology that aids organisations that build software and processes which leverage on data intensive business models to mitigate their privacy risks. These include risks related to regulatory compliance and end user privacy violation. This is achieved by delivering innovative solutions on methodology, tools and reporting of Privacy-by-Design in software-based systems. Our innovation helps technology based companies to save money through simplified regulatory compliance, increased productivity and to maintain brand reputation through embedded quality assurance.

Notes

PriSAT

Privacy Engineering for Software Designers

University of Glasgow

Contacts

Dr. Inah Omoronyia
inah.omoronyia@glasgow.ac.uk

prisat.org

The Privacy Tool

Bournemouth University

The Privacy Tool
Bournemouth University

Software that enables DPO roles to rapidly improve confidence in organisational Privacy Risk status

The Privacy Tool, a highly intuitive and visual privacy data discovery & assessment platform, has been created to respond to the immediate global need to enhance the maturity of information protection behaviour, and reduce the risk of cyber security breaches that may expose personal data.

Developed to implement the lead inventor's Privacy Throughout TM framework and methodology using its Privacy Logic Decision Engine the platform supports and actively guides Privacy Risk Assessment actions whilst building a detailed business context awareness. Any organisation looking to start or improve its privacy management posture can benefit from using The Privacy Tool. Designed to support organisational separation of duties and workflows with different levels of "personal data" handling it provides value to all users and facilitates a collaborative approach to privacy risk.

Notes

Contacts

Dr Jane Henriksen-Bulmer
jhenriksenbulmer@bournemouth.ac.uk
linkedin.com/in/janehb

cybersecurity.bournemouth.ac.uk

[INSURE]
SECURE WI-FI ACCESS

DE MONTFORT UNIVERSITY LEICESTER

INSURE
De Montfort University
Portable Wireless Intrusion Prevention Systems for Smartphones and Tablets

Public Wi-Fi is a cost-effective service used by 70% of tablet users and 53% of smartphone users. Unfortunately, security on public Wi-Fi networks is frequently non-existent or inadequate, exposing corporate data and personal information to sophisticated and untraceable threats. The use of security mechanisms, such as VPN, Unified Endpoint Managers, and Mobile Threat Defence tools, has become critically important for protecting end user devices. However, current security solutions manifest limitations with regards to adaptability, scope, and resources.

INSURE is a Portable Intrusion Prevention System, specially designed to protect Smartphones and Tablets against cyberattacks in public Wi-Fi networks. In contrast to existing solutions, the unique statistical engine at the core of INSURE enables unsupervised and adaptive real-time detection on the mobile device, without the need for cloud-based services or access to the Internet if the network is compromised by persistent threats. This software can be offered to end users as a standalone mobile app or embedded into existing security solutions.

Notes

[INSURE]
SECURE WI-FI ACCESS

DE MONTFORT
UNIVERSITY
LEICESTER

Contacts

Francisco Javier Aparicio Navarro
fnavarro@dmu.ac.uk
linkedin.com/in/francisco-aparicio-navarro

dmu.ac.uk

GuardKeeper
Coventry University
Advanced authentication and secure connections in hostile environments

95% of securely connected servers are vulnerable to man-in-the-middle attacks. The padlock in a web browser only indicates a secure connection, not who you are connected to. Even with using modern protocols, an attacker could be present within the connection.These types of attacks can lead to account compromises, and exposure to private and sensitive information.

Attacks on customers can cause a company to have bad press, and can lead to and reputation. Furthermore this can lead to a loss of customers and business. Our solution allows a user to not only establish whether they have a secure connection, but who they are connected with. This increases trust and security for the user, and will benefit the customer as they will have increased reputation for security for their users, and lower risk of security breaches.

GuardKeeper comes in two parts. The first part for the end-user comes as a web extension. This is convenient and efficient, and doesn't need technical knowledge to set up and use. It also provides the user with visual feedback which is clear and easy to understand. The second part is for developers of the company who buys our product. It is a simple to import and use code library which will allow for easy implementation.

Notes

Contacts

Dr James Shuttleworth
csx239@coventry.ac.uk
linkedin.com/in/digehode

Marcus Hill
marcus.hill1995@gmail.com
linkedin.com/in/marcusjhill

OnlynShield
University of Wolverhampton
Intelligent safeguarding software shielding children from harmful online communications

The Internet provides high exposure to malicious content with direct impact on children's safety such as Illicit, violent and pornographic material to name a few. Recent studies show the problem continues with 1 in 4 children exposed to racism or hate messages and over 2,200 counselling sessions with young people took place in 2017/18 related to online sexual exploitation which is a 44% increase from the previous year. Children are exposed to this risk both at home and at school. OnlynShield is a highly automated safeguarding software superseding the obsolete techniques in use today with an innovative and intelligent child-safety shield centred around a full prevent-strategy consisting of the following processes: "Identify", "Detect", "Assess", "Protect & Prevent". The value proposition is manifested by quicker intervention and better filtering capabilities with the ability to address emerging threats targeting children on social media. OnlynShield automates detection with enhanced Machine Learning algorithms, provide game-based education and awareness for children to develop their cyber resilience, and assess the risk to help parents and schools doing what is right and avoiding what is wrong.

Notes

OnlynShield
BE SAFE ONLINE

UNIVERSITY OF
WOLVERHAMPTON

Contacts

Dr Haider Al-Khateeb
H.Al-Khateeb@wlv.ac.uk
Twitter: @H4ider
linkedin.com/in/alkhateeb

Prof Amar Aggoun
A.Aggoun@wlv.ac.uk

onlynshield.co.uk | @OnlynShield

Prinesec
Royal Holloway
Creating causality chains to empower predictive threat detection

One in four organisations will experience a data breach within the next two-years. The primary reason behind the inability of existing solutions to efficiently detect and prevent a security breach is the delay in identification and containment of events across multiple sources.

PrineSec provides a solution that empowers organisations to efficiently and effectively respond to security incidents and map out and prevent the ones that are still unfolding. PrineSec does this by collecting together events as they arrive in log files, enriching them, and creating causality chains so that actions can be traced back to sources. Unlike other solutions in this space, PrineSec provides a full, condensed, and context-aware understanding of the events across systems. PrineSec uses these causality chains to recognise the potential of evolving events to cause damage – enabling an organisation to act and not just react. By doing this we empower staff and organisations to more effectively perform auditing of information security incidents, meet regulatory requirements, and increase the effectiveness of running a Security Operation Centre (SOC) along with the overall cybersecurity resilience of a company.

Our solution is developed within the renowned Information Security Group in Royal Holloway University of London. PrineSec started in April 2019; however, technologies underpinning PrineSec were developed during a three-year EPSRC funded project that will conclude in February 2020. Elements of this invention are currently under review as an international patent submitted by Royal Holloway, University of London.

Notes

PRINESEC
CONNECTING THE DOTS

ROYAL
HOLLOWAY
UNIVERSITY
OF LONDON

Contacts

Prof. Konstantinos Markantonakis
k.markantonakis@rhul.ac.uk
linkedin.com/in/kostas-markantonakis-3411a42

Freya Sheer Hardwick
www.linkedin.com/in/freya-sheer-hardwick

prinesec.com | info@prinesec.com

PhishAR
University of Oxford
Phish-proofing user authentication by harnessing the power of AI and AR.

Phishing attacks are present in more than a third of enterprise compromises and 83% of surveyed companies reported being exposed to phishing attacks in 2018. One potential countermeasure, often mandated by the GDPR, is two-factor authentication (2FA). However, neither using the existing smartphone applications, nor receiving codes via email or SMS provide protection against the latest rapidly increasing group of phishing attacks that specifically target 2FA users.
Our solution, PhishAR, is the only phishing-resistant second factor authenticator that runs on smartphones. The immersive intelligence of PhishAR uses machine learning and computer vision capabilities of modern smartphones to only provide the necessary log-in credentials if the user is visiting a legitimate website. Otherwise, as soon as a single individual gets exposed to new phishy content, PhishAR withholds their credentials and reports suspicious activity to the central AI system, thus allowing the organization to promptly neutralize a nascent attack campaign.

After patenting the core technology and developing a fully functioning implementation for Android smartphones, PhishAR is raising a seed investment and spinning-out from the University of Oxford. We are happy to report that one of the most significant multinational companies in the payments industry has already committed to be a non-lead investor in PhishAR and we are currently discussing the investment terms with several angel and venture capital investors. You can find more info at https://phishar.com. Speak to us if you can support us in this adventure!

Notes

Contacts

Professor Ivan Martinovic
ivan.martinovic@cs.ox.ac.uk

Dr Ivo Sluganovic
ivo.sluganovic@cs.ox.ac.uk
@ivosluganovic
uk.linkedin.com/in/ivosluganovic

phishar.com | @phishARcom | linkedin.com/company/phishar

BioGenerate
University of Gloucestershire and Imperial College London
Securing device to device communication

BioGenerate provides a robust solution for encrypting device to device communications. Whilst there are a number of applications, the most pressing market problems we address are in the medical and automotive sectors.

In the medical sector, BioGenerate encrypts the communication between medical implant devices and their external controllers thus reducing well-publicised vulnerabilities and improving patient well-being.

In the automotive sector, BioGenerate encrypts the communications in keyless entry/start systems thus preventing a ‘relay attack’ and theft of the vehicle.

BioGenerate is unique in that it harnesses the randomness in a person’s biological signals to encrypt communications between their devices e.g. key fob and vehicle, pacemaker and controller. Our ‘product’ is the IP to be able to perform this encryption and is sold under licence to manufacturers of the various devices.

BioGenerate is a collaborative research-based spin-out from Imperial College London and University of Gloucestershire.

Notes

biogenerate.it

UNIVERSITY OF GLOUCESTERSHIRE
at Cheltenham and Gloucester

Imperial College London

Contacts

Dr Hassan Chizari
hchizari@glos.ac.uk

Dr Martine Garland
mgarland1@glos.ac.uk

Dr Will Sayers
wsayers@glos.ac.uk

Prof. Emil Lupu
e.c.lupu@imperial.ac.uk

biogenerate.it

BLEMAP
Royal Holloway
Bluetooth security and vulnerability insight [in a blink]

Bluetooth connects billions of IoT devices today. A security issue in one of these devices can affect patients, allow a burglar into a home or be used as the entry point for an attack into a corporate network. Despite this, the security analysis of these devices today requires very specialised knowledge and professionals.

BLEMAP gives insight into what Bluetooth devices do and how secure they are. Our technology identifies security threats in a wide range of Bluetooth devices, enabling organisations to secure their wireless environments. BLEMAP is automatic, cost-efficient and effective and also allows security consultancy companies to save time and easily expand their range of services to Bluetooth security analysis.

Notes

BLEMAP

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Contacts

Dr Jorge Blasco Alis
Jorge.BlascoAlis@rhul.ac.uk
@guizos

blemap.com | info@blemap.com | @ble_map

Draconia
Bournemouth University
Cost-effective, bolt-on service for advanced threat detection

The performance of threat detection tools relies on the quality of their rules, but most companies lack the expertise to create them. Instead, their creation is either outsourced as part of an expensive bundle of managed services, which usually provides only basic rules, or is ignored. However, threat detection tools without proper rules are a waste of resources, which causes analyst fatigue, and leaves companies insecure.

Draconia brings to the market a dedicated bolt-on service that offers advanced and platform-agnostic detection rules. Our service provides up-to-date rules that enhance your security solutions, based on your industry, risks and needs. Better rules result in less false positives and therefore less analyst fatigue, so that your analysts can focus on the security alerts that matter.

Notes

DRACONIA

Bournemouth University

Contacts

Dr Alexios Mylonas
amylonas@bournemouth.ac.uk
linkedin.com/in/alexios-mylonas

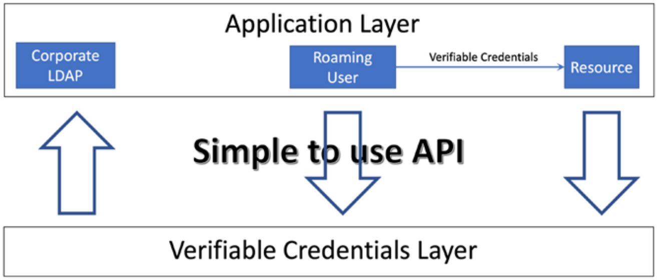
draconia.io

Verifiable Credentials

University of Kent

Replacing all credentials, including passwords, with W3C standardised, cryptographically-secured, electronic credentials.

We provide the virtual equivalent of physical credentials (plastic cards, passports, qualifications etc.) for everyone and everything so that they can easily identify themselves to anyone or anything, anywhere, at any time, by converting their credentials (including passwords) into cryptographically secure and privacy protecting W3C Verifiable Credentials. We provide an easy to use API so that all applications can quickly and easily integrate W3C Verifiable Credentials into their applications.



Notes

Verifiable Credentials Ltd

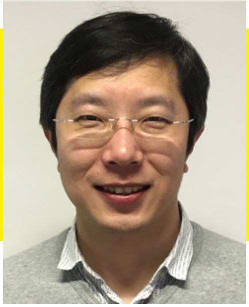
University of Kent

Contacts

Prof David Chadwick
d.w.chadwick@kent.ac.uk

Dr Ioram Sette
ioram7@gmail.com

verifiablecredentials.info | linkedin.com/company/verifiablecredentialsltd



TAPCHA

Bournemouth University

Online fraud prevention, CAPTCHA reinvented for everyone & every device

TAPCHA safeguards online services targeting the mobile market by improving the detection and prevention of non-authentic web traffic.

Our mission is to help everyone eliminate online fraud and maximise online transactions on mobile devices with an innovative human authentication solution that is not only easy to integrate with any platform but is also fully localisable and non-invasive for end users.

Notes

TAPCHA

Bournemouth University

Contacts

Nan Jiang
njiang@bournemouth.ac.uk

Huseyin Dogan

Angelos Stefanidis

http://tapcha.uk/wpdemo | @tapchauk

SPYDERISK UNIVERSITY OF Southampton

SPYDERISK
University of Southampton
Automated risk assessment for enterprise IT compliance

We make risk assessment of enterprise IT systems faster and more reliable for cyber security professionals. SPYDERISK's SaaS solution automates four processes: it finds all the threats in a system, following the web of attack paths; it calculates risk based on the threat likelihood and business impact; it proposes mitigations, drawn from a detailed knowledgebase; and finally, it generates the reports needed to get compliance certification. This is vital because right now such risk analysis is generally done manually and is therefore time-consuming and error-prone. SPYDERISK is based on 7 years' research at the University of Southampton and compared to similar tools uses more comprehensive models and has a better risk calculation. The value of the data in the model can be extracted not only into a "to do" list to give to a technical team but in the formats needed for ISO 27001 and SOC-2 compliance audits.

Notes

SPYDERISK

UNIVERSITY OF Southampton

Contacts

Dr Stephen C. Phillips
stephen.phillips@spyderisk.com

Prof. Mike Surridge
mike.surridge@spyderisk.com

Mr Niall Dickin
niall.dickin@spyderisk.com

spyderisk.com | info@spyderisk.com | linkedin.com/company/spyderisk | @SPYDERISK

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@ktn-uk.org	@CyberASAP linkedin.com/showcase/cyberasap