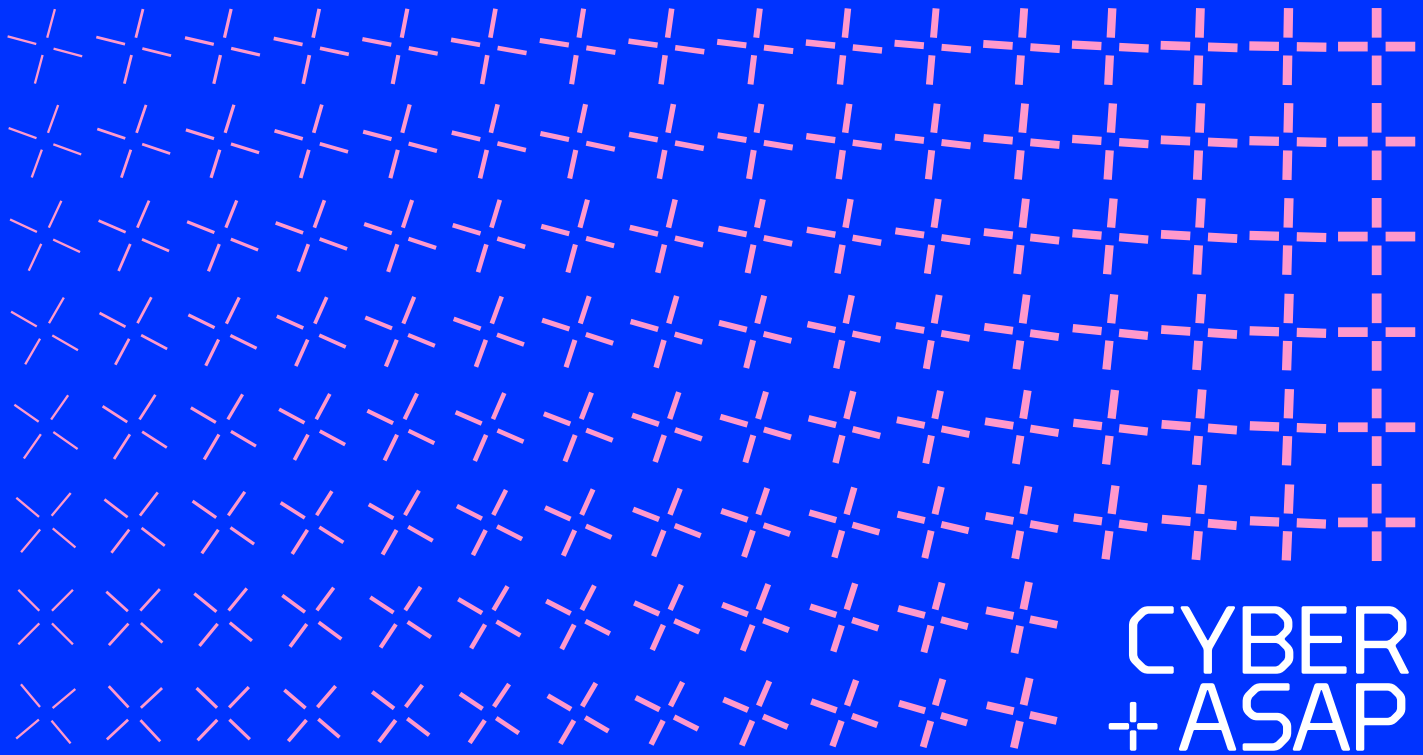
Cyber Security Academic Startup Accelerator Programme

Year 4 Demo Day + 18 February 2021



CYBER + ASAP

CyberASAP - Programme Context

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 work 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**
- **deter our adversaries and**
- **develop our capabilities.**

A crucial part of this is promoting the UK's cyber security sector, ensuring that 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 KTN.

> *"The CyberASAP programme plays an important role supporting academics to turn their research into market-ready products and it will not only help us build back better from the pandemic but also keep people across the country secure online."*
>
> **Matt Warman MP**
> Minister for Digital Infrastructure

Department for Digital, Culture Media & Sport

UKRI Innovate UK

ktn

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 fifth year, CyberASAP provides a comprehensive range of support to develop academics' entrepreneurial skills and convert their research into commercially viable 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.

Operating over three competitive stages, the programme is supported by external assessments and with input from highly experienced Knowledge Transfer Managers within KTN as well as from their expert connections within relevant industry sectors.

1A **Developing a Value Proposition**

1B **Market Validation of the Value Proposition**

2 **Developing of a Proof of Concept**

Outcomes

Further funding of more than £6m has been secured for "Alumni" of the programme to progress their projects. Successes come in many forms including: acquisition by technology firms; receiving seed funding; joining other accelerator programmes; securing government grants; partnering with commercial enterprises.

Looking ahead

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 as part of the government's £1.9billion national cyber security strategy.

In so doing CyberASAP provides a dynamic interface between government, cyber security academics and the business and investment communities so vital to the health and development of this sector.

For more information on how to participate in the programme visit cyberasap.co.uk

Event Running Order

Agenda

13.45 **Welcome:**
Dr Emma Fadlon, KTN

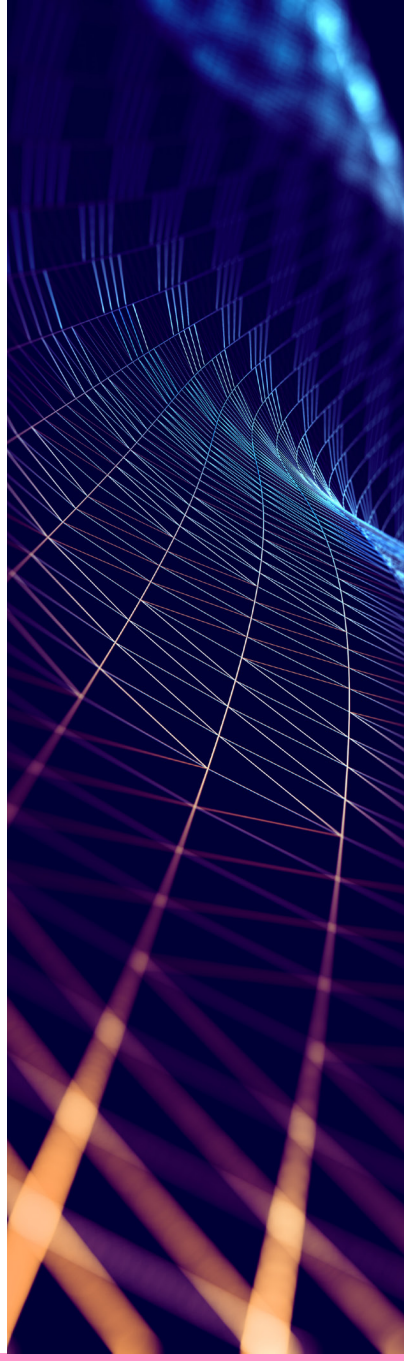
Pitches from CyberASAP Teams:
7 x 3 minute pitches; break; 7 x 3 minute pitches
(See running order for Team pitches on next page)

15.30 **Keynote:**
Matt Warman MP, Minister for Digital Infrastructure, DCMS

Ends 17.30 **Proof of Concept Demonstrations:**
Meet the teams and see their Proofs of Concept in their virtual booths

THANK YOU TO ALL OUR MENTORS & COLLABORATORS

CyberASAP is a collaborative enterprise, drawing on the experience and knowledge of KTN's Programme Directors, Emma Fadlon and Robin Kennedy, and their expert connections. This extended network of generous specialists who lend their expertise and insight is central to the success and impact of CyberASAP. *A huge thank you to all.*

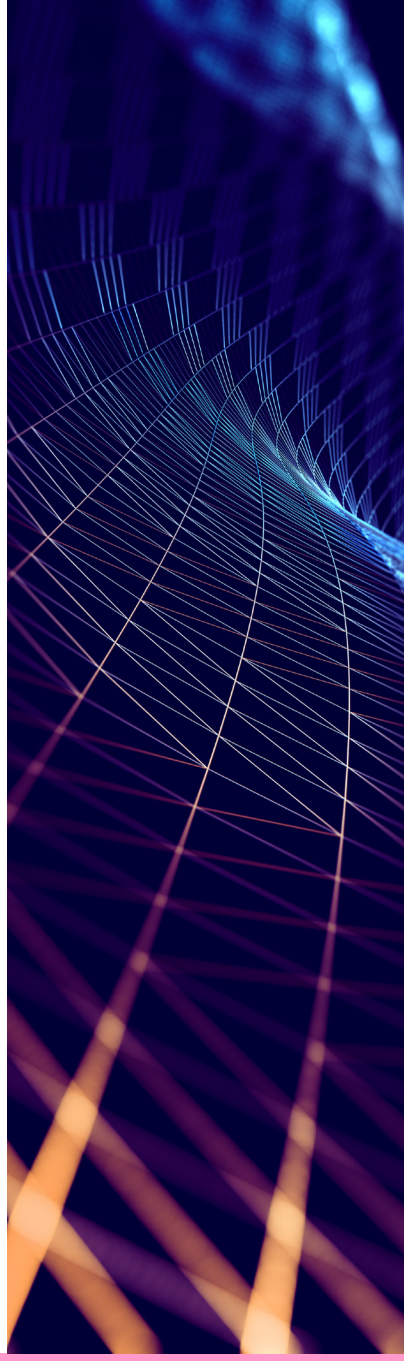


For more information on how to participate in the programme visit cyberasap.co.uk

Team Pitches Running Order

Our interactive menu can be clicked on:

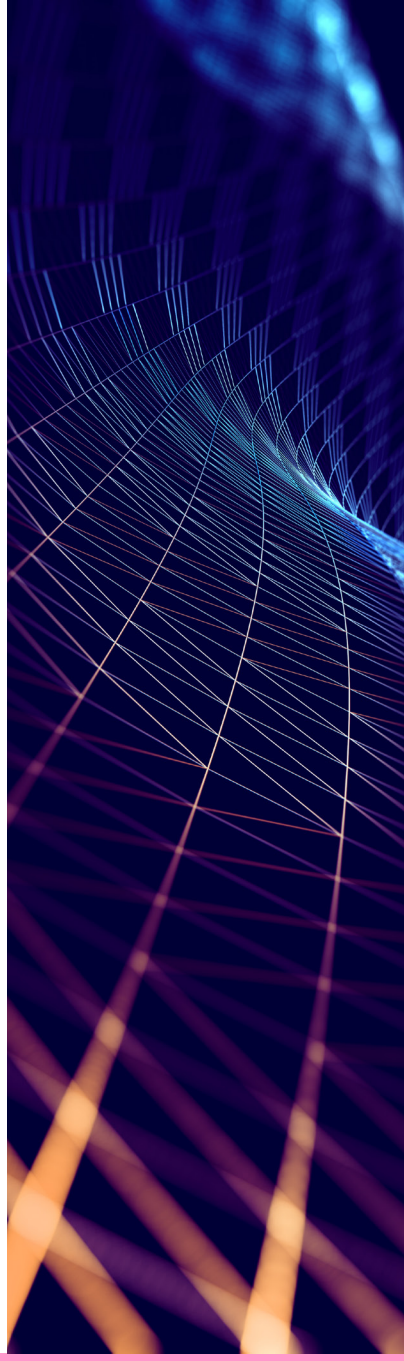
There will be a short break before the next 7 Team Pitches



For more information on how to participate in the programme visit cyberasap.co.uk

Team Pitches Running Order

Our interactive menu can be clicked on:



For more information on how to participate in the programme visit cyberasap.co.uk

Shoji

The safest way for businesses to buy and sell data

Jack Hogan

Jordan Noble

More and more businesses are looking to use external data to drive better decision making. However, due to data privacy and security concerns, accessing and evaluating even a single dataset can take months. Finding useful data is an extremely time-intensive, trial-and-error process.

To overcome today's compliance and onboarding barriers we are redefining the way that data is shared. The Shoji data exchange platform allows a data owner to license the use of their data, without that data having to be transferred outside of their own secure environment. A data buyer can perform analysis on the data in situ. Under the hood, a novel integration of federated learning and encryption techniques preserves privacy, ensuring identifying information is never exposed.

The team consists of statistical machine learning experts from Imperial College London with experience providing solutions for Microsoft, Barclays and Rolls Royce. We have received pre-seed investment from Entrepreneur First and are preparing to raise a seed round.

Contact Us

shoji.ai

Jack Hogan

jack.hogan15@imperial.ac.uk

/hogan-jack

Jordan Noble

jordan.noble10@imperial.ac.uk

/jordan--noble

Imperial College London

Authentibility Pass

An accessible authentication gateway for people with disabilities


Dr Paul Whittington


Dr Huseyin Dogan


Professor Keith Phalp


Lesley Hutchins

Authentibility Pass is a gateway that allows people with disabilities to communicate their authentication and accessibility requirements to organisations, including higher education institutions, schools, non-profit organisations and financial institutions.

The product comprises an Android application, database system, web interface and Application Programming Interface (API). Users enter their requirements into the Android application and complete authentication checks to verify the operation of a range of verification methods, including fingerprint detection and face recognition. Their requirements are then sent securely to organisations' databases. Each organisation can access their customers' requirements using a web interface with a search facility. Organisations with existing databases can use the API to export their customer requirements received from the Android application in a range of formats.

Using Authentibility Pass, customer requirements only need to be entered once into the Android application, which can then be sent to any number of supporting organisations. It is anticipated that Authentibility Pass will increase organisations' awareness of the requirements of their customers with disabilities as well as their compliance to legislations, including the Equality Act.

Contact Us

authentibility.com
@authentibility

Dr Paul Whittington
whittingtonp@bournemouth.ac.uk
/paul-whittington

Dr Huseyin Dogan
hdogan@bournemouth.ac.uk
/huseyin-dogan

Professor Keith Phalp
/keith-phalp

Bournemouth University

CyberHelper

Connecting machines and humans for efficient cyber investigations

Dr Erisa Karafili

Prof. Vladimiro Sassone

Our society is facing an increase in interconnectivity that comes with its own cybersecurity challenges. Security analysts analyze the data related to threats or cyberattacks, in order to put in place fast and efficient countermeasures. Frequently, the analysts find themselves overwhelmed with data to be analyzed and with tools that require a high level of expertise to be used. Both factors together with the time-pressure on the analysts, create a negative impact on the analysis and aggravate the already existing human-error element.

CyberHelper is a software solution for the analysis of threats and cyberattacks. This innovative tool combines network security, AI, and decision making, to guide security analysts during cyberattacks' investigations. CyberHelper improves the effectiveness of cyber analysis within an organization by connecting the knowledge, experience, and intuition of the cyber analysts to an extensible cyber intelligence knowledge base. CyberHelper improves the efficiency of cyberattacks investigations and reduces the investigation time.

Contact Us

cyberhelper.net
info@cyberhelper.net

Dr Erisa Karafili
e.karafili@soton.ac.uk
@ErisaKarafili
/erisakarafili

Prof. Vladimiro Sassone
vassone@soton.ac.uk
@v_sassone

University of Southampton

#ID / hash-identity

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


Gareth Howells


Klaus McDonald-Maier

Secure authentication is essential if users are to enjoy the benefits afforded by IoT systems, but the positive impact offered can't be realised while millions of IoT devices provide inadequate security and are susceptible to having their identity compromised.

IoT is fundamental in how technology can enhance our experiences, only possible when IoT devices can be trusted. #ID provides a unique form of device authentication, suitable for resource-constrained devices, where a unique identifier can be generated on demand 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.

Our team of academics is supported by respected industry professionals. The academics are recognised experts in their field, holding multiple patents & authored numerous papers. We have support from leading companies in the telecoms and semiconductor sectors.

Contact Us

hash-identity.com
W.G.J.Howells@kent.ac.uk

University of Kent

SurfaceRF

Making surfaces that identify, verify and protect themselves

Dr. Andrew Collins

Graham Marshall

Our technology determines the unique physical fingerprint of a surface using a patented form of surface radar. Surfaces protected by SurfaceRF technology are made physically and digitally verifiable. Protected enclosures and items are monitored actively or passively, depending on the desired application and a simple touch anywhere on the surface will trigger an alarm or simply log the event.

We provide the means to make enclosures tamper detecting over the entirety of their surface - with applications in cyber-security, the nuclear industry, defence and secure transit.

Contact Us

surfacerf.com
@SurfaceRF
Andy.collins@surfacerf.com
/andy-collins

University of BRISTOL

ABBA-IoT

Data tampering detection system for automotive sensors

Dr. Raoul Guiazon

Our mission is to detect cyber threats against vehicles.

Due to increased connectivity, vehicles are now more vulnerable to cyber-attacks. In 2015, two cyber-security researchers demonstrated the possibility to remotely take full control of a Jeep Cherokee, causing Fiat Chrysler to recall 1.4 million vehicles. That cost an estimated $0.5 billion and it is estimated that the cost of a single incident to the entire automotive sector could reach $24 billion by 2023.

ABBA-IoT is a data tampering and spoofing detection system that monitors the network of devices in a vehicle to detect anomalies in real-time. ABBA-IoT designs a dynamic pattern in the communication network of a vehicle through all legitimate sensors and devices that are monitored for attacks. In this way, any disruption by an intruder can be easily detected as abnormal.

In a constant race against cyber criminals, we aim to provide an Intrusion Detection System that gives our customers the peace of mind in knowing they are still ahead.

Contact Us

abbaiot.co.uk
@Abbalot

Dr. Raoul Guiazon
r.f.guiazon@leeds.ac.uk
/raoulguiazon
@RGuiazon

UNIVERSITY OF LEEDS

MEMCRYPT
Protect and Recover Your Most Important Secrets

MemCrypt

MemCrypt protects and recovers confidential data from ransomware attacks


Dr Owen Lo


Dr Peter McLaren


Prof Bill Buchanan


Dia Banerji

Ransomware blocks access to user data by locking it with an encryption key. The victim must pay a large sum of money (the ransom) to obtain this key in order to unlock and regain access to their own data.

Existing methods for combating ransomware include data backups, end-point protection, and cyber insurance solutions. However, these methods do not enable the user to quickly recover from an attack when ransomware has succeeded in encrypting user data.

MemCrypt has developed a framework which is capable of obtaining ransomware keys during an active attack. By acquiring the key, we are able to allow a user to immediately unlock and recover any data affected by ransomware. MemCrypt is also developing a ransomware incident reporting tool which provides a standardised approach to evidence gathering. Privacy preserving methods will be applied to enable sharing of ransomware attack data among digital investigators and stakeholders.

Contact Us

memcry.pt
@memcrypt

Dr Owen Lo
O.Lo@napier.ac.uk
/dr-owen-lo

Dr Peter McLaren
P.McLaren@napier.ac.uk
/peter-mclaren

Prof Bill Buchanan
B.Buchanan@napier.ac.uk
/billatnapier

Dia Banerji
Dia@memcrypt.io
/dia-banerji

Edinburgh Napier UNIVERSITY

CyberMIND Technology Ltd

An AI driven platform to help Cyber Professionals to Detect, Predict and Manage Stress


Ellen Kay


Prashant Pillai


Ali Sadiq

Cyber professionals are protecting our organisations and critical infrastructure. But stress is a growing problem due to a growing number of sophisticated cyber-attacks, shortage of skilled staff and overwhelming workloads. Recent studies have shown that 95% are working beyond their contracted hours and 48% are suffering from mental health issues.

To alleviate this problem, we have created CyberMINDtech - an AI driven platform to help 1) manage and predict your cyber team's mental health and wellbeing, 2) improve their performance and productivity and 3) reduce absenteeism and cyber risk.

The CyberMINDtech application can be installed on your smart phone or smart watch and will help you take control of your mental health with real-time stress monitoring, intelligent notifications and smart stress reducing interventions that can be automatically added to your daily calendars. Managers are also provided with anonymised organisational reports to improve corporate wellbeing and compliance with Duty of Care.

Contact Us

cybermindtech.com
info@cybermindtech.com
@CyberMindUK
/cybermind-technology-ltd

Secure Development

Helping consultants to make the 400,000 UK developers better at security

Charles Weir

Ingolf Becker

Secure Development is a revolutionary half-day package of structured workshops to motivate and empower developers to produce secure code, designed for non-specialist consultants and trainers to present.

An interactive game teaches that security is unthreatening and understandable; an ideation-based threat assessment session uncovers the relevant security and privacy needs of the developers' projects; and an analysis session makes security improvements saleable, by identifying business value for product management. Both online and face-to-face versions are available open source or can be rebranded for a fee.

A supporting system of online questionnaires measures the security capability of each team over time allowing certification of improvement; and supporting materials will include referrals to key partners.

Contact Us

securedevelopment.org
@Securedevelop

Charles Weir
c.weir1@lancaster.ac.uk
/charlesweir

Ingolf Becker
i.becker@ucl.ac.uk
/ingolf-becker

Lancaster University

SenseiChain

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

Ruhma Tahir

Klaus McDonald Maier

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.

Permissioned blockchain provides integrity, immutability and transparency; however it lacks in providing confidentiality that prevents enterprises from using blockchains to store sensitive data and exploring its true potential. Encryption of the blockchain data provides confidentiality but gives rise to issues such as lack of transparency, slow operations and inability to perform analytics on the data. Enterprises require a capability that enables monitoring and analytics to be performed on encrypted transactions, that ensures data transparency while preventing data loss.

In comparison to competitors SenseiChain offers both revolutionary blockchain capability and superior levels of scalability to improve the security and privacy, reduced network latency and enhanced efficiency. SenseiChain technology is currently being patented and will benefit different verticals including the banking sector, IoT, defence organizations, law enforcement agencies, healthcare domains and ecommerce sectors.

Contact Us

senseichain.com

Ruhma Tahir

rtahir@essex.ac.uk

/ruhmatahir

Klaus McDonald Maier

kdm@essex.ac.uk

University of Essex

LUPOVIS

Detect, Deceive, Divert, Deny, Identify


Xavier Bellekens


Christos Tachtatzis


Robert Atkinson


Ivan Andonovic

Lupovis provisions cyber-security deception solutions that use artificial intelligence to engage attackers on the onset of a breach. Lupovis creates dynamic deception environments maintaining the attacker on dynamically-defined paths away from valuable targets by adjusting the faux vulnerabilities of the solution. The data acquired is the basis to accurately characterise the attacker and associated strategies which then informs on the most effective countermeasure to arrest the attack, reducing the overall cost of successful cyber-attacks whilst facilitating an investigation of the breach.

The Lupovis deception engagement is implemented by establishing a 'narrative' embedded with manipulation and gamification methodologies. The 'narrative' keeps the attacker on dynamically-defined paths and the 'gamification' of the decoy element of the solution optimally aligns and adapts vulnerabilities to the skills of the attacker. Thus the system automatically adjusts its mix of deceptions features depending on the sophistication and skills of the hacker.

Contact Us

lupovis.io
@LupovisDefence
/lupovis
xavier.bellekens@strath.ac.uk

University of Strathclyde Glasgow

SALMAC

Linux Threat Hunting Solution

Dr Mahdi Aiash

Prof Jonathan Loo

SALMAC is a unique security assessment tool focusing on hardening Linux access control systems in order to reduce the attack surface and to stop misconfiguration-based attacks in Linux environment. It uses a threat model based on the MITRE ATT&K Framework to simulate attacks targeting Linux systems.

Whilst simulating these attacks, it pulls logs entries from the targeted machines and links them to the launched attacks in order to produce attacks' signature. Once identifying the misconfiguration in the system, SALMAC will then apply the needed remediation to harden the tested system and block the attacks. SALMAC not only runs as a stand-alone service, it can also integrate into existing solutions to complement their offerings and hence addressing the gap of existing security assessment tools.

Contact Us

Dr Mahdi Aiash
M.Aiash@mdx.ac.uk
@DrAiash
/dr-mahdi-aiash

Prof Jonathan Loo
/professor-jonathan-loo

Middlesex University London

WhatML

WhatML

Watermarking for protecting the value and the intellectual property of machine learning models

Dr Luis Muñoz-González

Prof Emil C Lupu

Designing and deploying machine learning models is expensive: They require a large amount of data, computational resources, time and expertise to be trained and deployed. Machine learning models are thus hugely valuable assets. In a growing market, with different opportunities to monetise these models at the moment, there are no solutions to protect their value. Machine learning models are thus often exposed and can be stolen or used beyond the agreed scope of use. This can produce significant losses for many businesses and impede the growth of machine learning markets.

Our team at Imperial College London have developed WhatML, a solution to protect the intellectual property of machine learning models through watermarking. WhatML allows to introduce watermarks in the models and includes mechanisms to verify the model's ownership and provenance by checking that the watermarks are present. Our watermarks are resistant to different transformations and do not impact the system's performance.

Contact Us

Dr Luis Muñoz-González
l.munoz@imperial.ac.uk
/lmunoz-gonzalez

Prof Emil C Lupu
e.c.lupu@imperial.ac.uk
/emillupu

Imperial College London

MaCRA

MaCRA provides dynamic, multi-dimensional risk assessment tooling that uniquely addresses both IT and OT elements of a specific vessel system, by factoring in threat associated with both the cargo transported and the route operated


Kevin Forshaw


Kimberly Tam


Kevin Jones

We uniquely provide dynamic assessment of maritime cyber threat, for both Individual vessel operators and organisations, by providing operational-specific, multi-dimensional risk assessment tooling, because Maritime Cyber incidents occur on a daily basis threatening both safety and operations costing many £millions in recovery.

There are just under 180,000 ships alone in Global Fleet but these figures do not factor in the many more fishing boats, navy vessels and superyachts that MaCRA is equally applicable to. The market for MaCRA is also becoming regulatory driven, with IMO Guidelines mandating all operators to conduct maritime cyber risk assessment in 2021. But currently, tools for maritime risk assessment don't exist. Our extensive network of senior level security leads in many operators convey a reoccurring theme of IT consultants proposing solutions that are not fit for purpose.

Contact Us

plymouth.ac.uk/research/maritime-cyber-threats-research-group

Kevin Forshaw
kevin.forshaw@plymouth.ac.uk

Kimberly Tam
Kimberly.tam@plymouth.ac.uk

UNIVERSITY OF PLYMOUTH

Cyber Security Academic Startup Accelerator Programme

CyberASAP Programme Directors

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

Dr Emma Fadlon
Investment
emma.fadlon@ktn-uk.org
+44 7964 551643

CYBER + ASAP

cyberasap.co.uk
@CyberASAP
cyberasap@ktn-uk.org
/cyberasap

ktn

ktn-uk.org
@KTNUK