CYBER + ASAP | Academic Startup Accelerator Programme

Demo Day Programme 22/23

22 February 2023
Level 39, Canary Wharf
London

CyberASAP - Programme Context

The Department for Science, Innovation and Technology (DSIT) is leading the government's work to develop the world's best and most secure digital economy. DSIT wants the UK to be the best place to start and grow a business.

The National Cyber Strategy is the Government's plan to ensure that the UK remains confident, capable and resilient in this fast-moving digital world; and that the UK continues to adapt, innovate and invest in order to protect and promote our interests in cyberspace.

This strategy delivers on a commitment made in the government's Integrated Review of Security, Defence, Development and Foreign Policy.

Department for Science, Innovation & Technology

UKRI Innovate UK

UKRI Innovate UK KTN

The 5 Pillars

The Integrated Review set out five 'priority actions' which form the pillars of the UK government's strategic framework, guiding and organising the specific actions we will take and the outcomes we intend to achieve by 2025.

Pillar 1

Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry.

Pillar 2

Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected.

Pillar 3

Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies.

Pillar 4

Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power.

Pillar 5

Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers.

CyberASAP is funded by DSIT and delivered in partnership with Innovate UK (grant funding to universities) and Innovate UK KTN (programme delivery). In 2021 CyberASAP introduced a new funding stream for PETRAS projects, part of the Security of Digital Technology at the Periphery programme (SDTaP) funded by UKRI.

Expanding Skills

The only pre-seed accelerator programme in the UK's cyber ecosystem, CyberASAP helps convert great academic research into great cyber innovations. The programme provides a dynamic interface between government, cyber security academics and the business and investment communities that helps drive the growth and development of this key sector.

Led by a highly experienced team from Innovate UK KTN, with input and assessment from their expert industry connections, CyberASAP operates over two competitive stages, (see right).

PHASE 1

Developing a Value Proposition

Market Validation of the Value Proposition

PHASE 2

Creating a Proof of Concept

Driving Innovation

Commercial upskilling; an entrepreneurial mindset; exposure to new business concepts and language; advanced market research and comms techniques; insights into how investors think and work; honing effective presentation techniques - just some of the takeaways designed to give talented academics the confidence and know-how to translate their research into viable cyber products, technologies and services.

There's no single pathway for the talented academics who participate in CyberASAP. But what unites them is the value they draw from being on the programme: the knowledge gained can enrich their ongoing work either within academia or industry, creating more opportunities to extend the impact of their experience.

Our Alumni have secured more than £19m in further funding to progress their projects. Successes come in many forms including: creating start ups (27 to date); acquisition by technology firms; receiving seed funding; joining other accelerator programmes; securing government grants; and partnering with commercial enterprises. Read our Impact Report and Case Studies at cyberasap.co.uk.

Event Running Order

01

Alumni Spinout Showcase and Registration

Meet with selected CyberASAP Alumni over lunch

02

Welcome

Dr Emma Fadlon, Co-Director, CyberASAP, Innovate UK KTN

03

Keynote

Erika Lewis, Director of Cyber Security & Digital Identity, DSIT

04

Pitches from CyberASAP Year 6 Teams and Break

See running order for Team pitches on next page

05

Year 6 Showcase/Demos, Networking and Drinks

Meet with the teams and discuss their proof-of-concept demonstrations

Team Pitches Running Order

01. **Lasting Asset – Edinburgh Napier University**
    Protecting crypto assets with the latest in custody technology
02. **MoFish – Oxford Brookes University**
    Connecting IT systems to cloud services with cyber-safe technology
03. **DRS'OSA – University of Salford**
    The holistic security solution ensuring cyber-resilient railway systems
04. **GICAST – The Open University**
    Delivering lasting cyber security behavioural transformation for businesses
05. **ROS-PCon – University of West London**
    Protecting industrial robotic systems from cyber-physical attack
06. **ANTHEM – Loughborough University**
    Rapid and autonomous threat modelling using innovative AI technology
07. **CyGamBIT – Bournemouth University**
    Interactive cyber security games helping young people to stay safe online
08. **Mindgard – Lancaster University**
    Specialist cyber security software and consultancy for AI-enabled businesses
09. **CLADDED – University of Warwick**
    Detecting and deterring attacks on electric vehicle charging points
10. **CASPER Shield – Cardiff University**
    Providing cyber-physical security and safety for smart homes
11. **Hacktivity Cybersecurity Labs – Leeds Beckett University**
    Providing safe environments for hands-on hacking and cyber security education
12. **D-PRIV for Safer Data – Teesside University**
    Data anonymisation software to help businesses protect confidential information
13. **ATDPS – University of Sheffield**
    The unique security solution protecting businesses from zero-day trojan attacks
14. **D-RON – Queen's University Belfast**
    Detecting and preventing rogue drone behaviour using digital twins
15. **IoTrim – Imperial College London**
    Making IoT device connections secure with privacy-preserving AI

LastingAsset

Protecting crypto assets with the latest in custody technology

Market Need

Despite some $140 million worth of crypto being lost as a result of failing custody approaches, investors are still paying a fortune for services which are costly, inflexible and inaccessible. Storing the private keys of these digital assets is challenging, making crypto asset security a huge concern.

Current technologies include Multi-Signature, Hardware Security Module (HSM) devices, and Multiparty Computation (MPC). While HSM-based wallets suffer from accessibility issues and risk too much manual intervention, MPC and Multi-Signature wallets aren't flexible enough or are too complex to implement.

Solution

LastingAsset proposes a novel, highly-secure, cost-efficient and convenient crypto assets custody platform. Using cutting-edge technologies, it provides peace of mind to investors, keeping assets safe and accessible. Multi-layer security, innovative backup and recovery mechanisms, and no single point of failure are just some of the benefits of this innovative system.

Others include full key ownership, non-custodian and custodian options, as well as enforceable and flexible governance policies. LastingAsset is also decentralised, scalable and compliance ready, using simple, trusted, execution environment technology for key generation, with full accountability.

Target Market

- Crypto asset investors/owners
- Companies producing crypto assets e.g. for luxury goods
- Future plans to support law firms in document security

Status & Needs

- Prototype ready spring 2023
- Aiming to deliver pilot project
- MVP delivery mid-late 2023

Team from Edinburgh Napier University

Dr Zakwan Jaroucheh
CTO and Lecturer

Dr Baraq Ghaleb
System architect and Lecturer

Prof Bill Buchanan
Cryptographic researcher and Professor

Nanik Ramchandani
CEO and Entrepreneur

Contact details

Email: hello@lastingasset.com
Website: lastingasset.com
Twitter: @LastingAsset
LinkedIn: /lastingasset

MoFish

Connecting IT systems to cloud services with cyber-safe technology

Market Need

SMEs frequently need to update their IT stack with new data, analytical systems and assessment elements to test and evaluate new approaches and technologies. Yet over 60% of small software integration projects are severely delayed due to a lack of software developers.

The number of AI solutions and services in the cloud are rapidly expanding, so companies are increasingly needing to connect to these services. A common way of solving this is to go to the IT department — but with so many requests, delays are inevitable.

Solution

A solution is needed to make connecting these systems easier and safer, instead of people just accepting systems as is. Current solutions are heavyweight tools requiring expensive specialists, lightweight tools requiring substantial software knowledge, or low-code tools requiring an entire IT-system architecture change.

MoFish is a web app that allows people to register web services and connect them visually. It enables those with limited technical knowledge to add new cloud-based IT services. Cyber security measures will also be embedded, making it easy for users to stay alert to potentially dangerous connections.

Target Market

- Companies using cloud-based IT services
- Businesses seeking unique data sources
- IT systems managers

Status & Needs

- Prototype in testing
- Have funding from university for MVP
- Seeking industry feedback on beta version

Team from Oxford Brookes University

Kevin Maynard
Principle Investigator and Co-Director at Institute for Ethical AI

Mohamed Mohamed
Project Researcher and Senior Post-Doctoral Researcher

Ivan Fursa
Software Engineer

Contact details

Email: ethicalAI@brookes.ac.uk
Website: www.ethical-ai.ac.uk

DRS'OSA

The holistic security solution ensuring cyber-resilient railway systems

Market Need

The digitisation of rail systems allows for improved capacity, traffic management, reliability and energy efficiency. However, although we haven't yet seen a cyber attack on train control systems, researchers in this area have identified threats and the need to come up with a solution before the digitisation of our rail systems is complete.

Existing security research solutions include hardware security, model-based security, and offline security learning systems. However, we currently lack a comprehensive security solution with humans involved in the operation cycle.

Solution

A real-time security monitoring and management system is required, one that doesn't simply offer a hardware-based solution or pure detection algorithm. DRS'OSA offers on-board detection and real-time incident management, reducing the risk or damage of a cyber attack.

DRS'OSA also provides multi-channel monitoring and an adaptive anomaly detection system. It delivers fast response and fast recovery by linking with the digital twin of the railway operation centre, and puts humans in the operation cycle to provide the bridge between cyber attack information and cyber incident management.

Target Market

- Rail industry - existing links with East West Rail
- Future plans to connect to energy industry

Status & Needs

- Currently working on Proof of Concept
- Hoping for industry approval and recognition of need

Team from University of Salford, De Montfort University, University College London and Keele University:

Dr Hongmei 'Mary' He - Project Lead, Professor of Future Robotics, Engineering & Transport Systems

Jeremy Watson - IoT, Cyber Security & Safety, Edge Systems

Prof Eerke Boiten - Cyber Security, Privacy, Cyber Intelligence Sharing

Dr Uchenna Ani - Cyber Security and Human Factors

Contact details

Email: h.he5@salford.ac.uk

GICAST

Delivering lasting cyber security behavioural transformation for businesses

Market Need

95% of cyber security breaches are a result of human error, yet the cyber security awareness programmes currently available to businesses offer no real evidence or insight into the security behaviours of the workforce.

In order to reduce the risk from human error, employers need insight into the individual attitudes and behaviours of their workforce. At present, this type of data is not available and the majority of cyber security awareness training methods are merely a tick-box exercise and offer no demonstrable reduction in risk.

Solution

GICAST is a game-based cyber behaviour assessment and skills training platform, offering businesses insight into employee behaviour through the power of game mechanics and learner behavioural analytics.

This solution helps businesses reduce security risks and threats due to human-factors, increase compliance with security policies and protocols, and create long-lasting behavioural change. It will also help them apply the right levers to enhance their security posture and optimise their time, effort and budget, making strategic decisions and focusing on the right areas of their business, while maintaining their reputation.

Target Market

- Businesses with cyber security training requirements
- Critical infrastructure sector
- Government organisations

Status & Needs

- PoC complete - already have early adopters
- Looking to deliver an impact evaluation report
- Seeking angel investment to develop MVP

Team from The Open University

Dr Chitra Balakrishna
Project Lead, Cyber Security Programme Lead

Contact details

Email: chitra.balakrishna@open.ac.uk
Website: open.ac.uk/gicast
LinkeIn: /chitra-balakrishna

ROS-PCon

Protecting industrial robotic systems from cyber-physical attack

Market Need

Despite the huge benefits robotics brings to many businesses, there's also a constant risk of attacks on the industrial robotic operations, especially as the robotics space moves towards autonomy in so-called 'smart factories'. Industrial robots are widely integrated within the network ecosystem for remote interaction, leaving them compromised through system vulnerabilities, misconfigurations and insider attacks.

Whilst there are products that focus on the security hardening of the robotic system — providing front-line defence — the industry is yet to deliver a real-time anomaly detection and prevention system.

Solution

ROS-PCon stands at the second line of defence, analysing problems such as changing of robot operation, behavioural anomalies, machinery health and safety, and the risk to robotic operators. By learning the robotic movement in a best-case environment, ROS-PCon can highlight anomalies when it spots something unusual.

The system helps expose any stealthy hacking activity, but can also serve health and safety purposes too. Anomalies may also be caused by technical malfunctions or failures, which ROS-PCon can detect before these break down or cause potential harm to workers.

Target Market

- Industry 4.0 Manufacturing & Automation
- Nuclear Robotics
- Biomedical Robotics

Status & Needs

- Proof of Concept complete
- Moving to business development and beta-testing
- Seeking funding to continue development of MVP

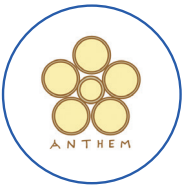
Team from University of West London

Professor Jonathan Loo
Project Lead and Technical Innovator

Professor Wei Jie
Co-Project Lead & Senior Researcher

Contact details

Email: jonathan.loo@uwl.ac.uk
Website: ros-pcon.herokuapp.com
LinkedIn: /ros-pcon



ANTHEM

Rapid and autonomous threat modelling using innovative AI technology

Market Need

Nearly half of UK smart manufacturers have been targeted by cyber threats, with attacks increasing and diversifying thanks to rapid asset digitisation. Despite this, security analysts are still relying on manual processes to investigate and devise attack scenarios.

Manual threat modelling processes are slow, taking 56 days on average – and up to 700 days in 12% of cases – to identify exploited vulnerabilities. Not only does it take time, but the mitigation actions generated are usually generic and difficult to put into context for individual companies.

Solution

ANTHEM is the only AI solution that rapidly and autonomously generates attack graphs for threat modelling. It utilises an innovative technology to prioritise mitigation actions quicker and cheaper than any of its rivals.

This system adapts to environmental changes in an iterative and autonomous way in order to identify paths that an attacker may take to reach a critical asset, by combining threat scenarios and risk profiles. It prioritises threats based on their criticality and likelihood, as well as mitigation controls within acceptable time frames.

Target Market

- UK-based smart manufacturers and critical infrastructure organisations
- Automotive and Pharmaceutical
- Security solution providers within Industry 4.0

Status & Needs

- Hope to have AI component complete by end of Feb
- Need support to form business development plan
- Seeking investment from angel investors and seed funding

Team from Loughborough University & University of Warwick

Dr. Kostas Kyriakopoulos - Senior Lecturer in Digital Communications

Dr. Gregory Epiphaniou - Associate Professor of Security Engineering

Dr. Iain Phillips - Senior Lecturer in Computer Science

Prof. Carsten Maple - Professor of Cyber Systems Engineering

Contact details

Email: K.Kyriakopoulos@lboro.ac.uk

Website: theron-defence.co.uk/intro/

LinkedIn: /kostas7

CyGamBIT

Interactive cybersecurity games helping young people to stay safe online

Market Need

There are currently 10.7 million young people aged 10-24 in the UK facing risk online. While 84% of parents say they worry about their child's online safety, on average they spend just 46 minutes talking to them about it.

The NSPCC stresses that talking regularly with children is the greatest tool to help keep them safe online. However, these conversations aren't happening, with almost three-quarters of parents and teachers having never received any guidance on supporting young people with online privacy.

Solution

CyGamBIT is designed to facilitate these complex conversations before issues arise, fusing high-quality cyber security and privacy education with a live-service, dynamic game that equips young people for a digital world. Its adaptability also ensures that learning is responsive to ever-evolving cyber security threats.

The CyGamBIT team have worked with young people and parents/guardians to develop the product, aligning with the National Cyber Strategy to cover the primary areas of concern. These include cyber bullying, self-identity, privacy, security, scams and phishing.

Target Market

- Academy schools sector
- Educators looking to teach financial literacy

Status & Needs

- Prototype in development
- Seeking funding to develop full, not-for profit platform

Team from Bournemouth University

Emily Rosenorn-Lanng
Principal Investigator & Research Project Officer

Stefan Kleipoedszus
Programme Leader & Deputy Head of Department

Stevie Corbin-Clarke
Research Assistant

Contact details

Email: cygambit.bu@gmail.com
Website: cygambit.co.uk
Twitter: @CyGamBITUK

Mindgard

Specialist cyber security software and consultancy for AI-enabled businesses

Market Need

Artificial intelligence is an aggressively expanding market and is delivering high value within many businesses. But such technology leaves them vulnerable to adversarial attacks, including those not solvable by firewalls or encryption. This can cause loss of financial and market position, GDPR fines and reputational damage.

Performing cyber risk assessment of AI technologies is difficult and expensive. It requires many years of training in AI and cyber, so there's a skills shortage and limited talent pool. With no best practice and a rapidly-changing landscape, a solution is needed.

Solution

Mindgard is a Deep Tech company offering specialist cyber security B2B software and consultancy services. The aim is to provide a quick, intuitive, jargon-free software solution that reduces the risk analysis process from months to minutes. The system will allow users to rapidly design, analyse and report AI technology cyber risk against thousands of state-of-the-art scenarios.

Mindgard aims to speed up the process of AI assessment, compressing 6-9 months of work into 60 seconds. It runs real threat scenarios and full-stack attacks, delivering significant time and cost savings.

Target Market

- AI-ready businesses
- Technology and defence sectors
- Enterprise AI creators and consumers

Status & Needs

- Software works and delivers value
- Seeking investors to help grow into a company
- Already have interest from several investors

Team from Lancaster University

Prof. Peter Garraghan
Project Lead and Professor of Computer Science

Prof. Neeraj Suri
Distinguished Professorship and Chair in Cybersecurity

Contact details

Email: p.garraghan@lancaster.ac.uk

CLADDED

Detecting and deterring attacks on electric vehicle charging points

Market Need

As demand for electric vehicles continues to increase, so too does the need for electric charging points. But now there's an additional requirement to secure electric car charging stations and protect them from cyber threats, particularly those used with smart devices.

Current methods rely on end-to-end encryption which isn't an ideal solution for EV charging points and cannot be implemented in old devices. With new government regulations dictating that all charging stations must be compatible with smart devices, the need to secure them is greater than ever.

Solution

Researchers at the University of Warwick recognised the need for a tailor-made solution - one that was more accurate but lower cost. They created CLADDED: a data-driven online behaviour-monitoring software framework, designed specifically for EV charging points.

This cross-layered, data-driven system is designed to detect and deter attacks on electric vehicle charging stations. It offers cutting-edge, artificial intelligence-based solutions for charging firms that seek to secure their charging points. Unlike encryption-based solutions, CLADDED is scalable and easy to integrate into both new and existing EV charging points.

Target Market

- Electric vehicle charging point providers
- Also scope to target the National Grid

Status & Needs

- Back-end of product complete
- Seeking investment and engineer support

Team from Warwick University

Hamidreza Jahangir
Project Lead and Research Fellow, Machine Learning

Subhash Lakshminarayana
Associate Professor, Power Grid Security

Carsten Maple
Professor, Cyber Systems Engineering

Tim Francis
TTO, Business Development

Contact details

Email: Hamidreza.Jahangir@warwick.ac.uk

Website: sites.google.com/view/cladded

LinkedIn: /cladded

CASPER Shield

Providing cyber-physical security and safety for smart homes

Market Need

Smart homes contain programmable electronic devices that enable home automation and interconnectivity. However, conventional home security or network protection systems focus on purely cyber or physical events, rather than a combined approach, meaning they fail to detect certain intrusions.

The need to protect smart homes against these types of attacks is increasing. Traditional security systems are either network or physical-based, but currently, no one is offering a combined solution. Should front-line security systems fail, smart homes would be left vulnerable, so a more resilient, complementary solution is needed.

Solution

CASPER Shield looks for abnormal occurrences using first-hand cyber and physical data rather than relying on insecurely transmitted, manipulable second-hand data. It deploys AI-based algorithms to discover anomalies in real time, based on the behaviours of devices and occupants.

This novel system aims to protect you and your connected things from criminals and make connected living spaces more secure and safe. The approach is built on edge computing, ensuring end-user data security and confidentiality to ensure maximum privacy.

Target Market

- Internet Service Providers
- IoT smart home ecosystem manufacturers
- End-users will be smart home owners

Status & Needs

- Proof of concept complete
- Working on business development and R&D
- Seeking partner with whom to run a pilot

Team from Cardiff University

Dr Charith Perera
Project Lead and CEO

Yasar Majib
CTO and PhD Researcher

Hakan Kayan
CSO and Research Student

Contact details

Email: pererac@cardiff.ac.uk
Website: charithperera.net

Hacktivity

Providing safe environments for hands-on hacking and cyber security education

Market Need

The need for training cyber security professionals is unavoidable and more pressing than ever. In the past year, almost half of all cyber sector firms have faced skills gaps, thanks to huge shortfalls in skilled individuals.

Current hacking platforms or cyber security education tools offer a typically poor desktop experience and limited tracking of skills development. In addition, they are vulnerable to cheating and only offer manually-created, static challenges which are only suitable for one-time use. The market is undergoing extreme growth, and needs a more up-to-date solution.

Solution

Hacktivity is different from competitors, thanks to a code-based approach that generates new scenarios and challenges each time you access the platform. This helps solve problems of plagiarism and provides real-life systems to practise attacking. The platform offers realism, depth and industry relevance not seen in any other systems.

It also provides continuous development, with randomisation offering endless combinations of possibilities. It aims to deliver cyber security education in a fun and safe space, where students, hobbyists and enthusiasts can learn through doing.

Target Market

- B2C end consumer interested in developing skills
- B2B businesses with training requirements
- Businesses who need platforms to deliver training

Status & Needs

- Live system already being used by hundreds of students
- Developers hired to progress to market in 2023
- Exploring options for investment

Team from Leeds Beckett University

Dr Z. Cliffe Schreuders
Project Lead, Reader in Cyber Security and Director of the CSI Centre

Julian Farrell
Business Development Manager

Contact details

Email: c.schreuders@leedsbeckett.ac.uk

Website: hacktivity/leedsbeckett.ac.uk

D-PRIV for Safer Data

Data anonymisation software to help businesses protect confidential information

Market Need

60% of SMEs use a data-driven approach to boost their processes, drive strategies, and improve their financial performance. Keeping confidential information should be a top priority for these businesses and it's more critical than ever that data meets GDPR requirements.

But data anonymisation services can be expensive, require a high level of skills and be difficult to deploy, making them inaccessible. Working in the digital health sector was the inspiration for project lead Dr Jie Li, who found issues with data anonymisation when developing patient monitoring software.

Solution

D-PRIV looks to address current challenges through a data anonymisation system which protects data and avoids the risk of compromising confidential information. It allows various sites to communicate with the central controller to help manage their privacy model without sharing any sensitive information.

The team have developed several privacy models to deal with different types of data including healthcare and digital medical imagery, addressing issues of cost, deployment and required skill level. For businesses who need to work with real data, this kind of anonymisation is vital.

Target Market

- Healthcare industry
- Research & academia
- SMEs using data-driven approaches

Status & Needs

- Ready to launch first alpha test model early 2023
- Seeking feedback from the digital health community
- Looking for investment and support (e.g. marketing)

Team from Teesside University

Dr Jie Li
Project Lead, Senior Lecturer and Expert in Data Science

Dr Mohammed Abdur Razzaque
Associate Professor, Expert in IoT & Cyber Security

Contact details

Email:
jie.li@tees.ac.uk
m.razzaque@tees.ac.uk

ATDPS

The unique security solution protecting businesses from zero-day trojan attacks

Market Need

At present, the majority of large IT vendors invest in developing private security systems for their projects which — due to a failure to detect and mitigate zero-day trojans — leaves them vulnerable to breaches.

Whilst existing solutions make use of the Trojan Detection System, capable of mitigating known trojan signatures, there is currently no solution to combat unseen attacks. These solutions use firewall, cryptography, Automotive Penetration Testing and Authenticated frame transmission. However, they lack adaptivity, and are both expensive and resource exhaustive.

Solution

The team behind ATDPS seek to be the first in the market to provide significant protection against zero-day trojans, with a long-term ambition of providing security throughout the entire phase of an IC (integrated circuit) supply chain.

Their unique system provides a lightweight, adaptive and inexpensive solution with resilience against unknown trojans and scalability. It focuses on two areas: a Machine Learning (ML)-based approach for Trojan Detection and Prevention System and a Physically Unclonable Function (PUF)-based hardware protection system.

Target Market

- Fabless manufacturers
- SMEs with interest in this area
- Targeting autonomous vehicle industry as entry to market

Status & Needs

- MVP completed by mid-February 2023
- Working on packages with two different partners
- Seeking support from automobile/ hardware security industries

Team from University of Sheffield

Dr Prosanta Gope
Lecturer and Assistant Professor in cyber security

Aryan Mohammadi Pasikhani
Former PhD student and project mentor

Soumadeep Das
Research Assistant, Cybersecurity & Artificial Intelligence

Owen Millwood
PhD student, resource-constrained security and PUFs

Contact details

Email: p.gope@sheffield.ac.uk
Website: sites.google.com/view/prosantagope
ATDPS Website: atdps4noc.website2.me
LinkedIn: /atdps

D-RON

Detecting and preventing rogue drone behaviour using digital twins

Market Need

The drone sector expects huge growth over the next five to ten years. However, through extensive research and market validation, experts in cyber technology at Queen's University Belfast have identified market needs and potential fears, including a significant risk of collateral damage.

Attacks on drones are relatively easy to carry out, thus providing a need to investigate any potential attacks as well as detect and prevent them. Existing approaches rely on expensive technology and heavy equipment, both complex to deploy and unable to distinguish threat type.

Solution

D-RON leverages AI and digital twin technology to deliver a resilient, cost-effective platform that offers swarm movement detection, pattern tracing and individual movement tracking of drones. It will also provide better observation and reporting, faster response times, and fewer false positives.

The technology offers real-time anomaly detection as well as group authentication, self-checking logic and peer-to-peer observations. This solution could be useful in investigating whether drone swarms have fallen victim to cyber attack.

Target Market

- Anti-drone companies
- Military and commercial
- Building owners who want to avoid drone fly-overs

Status & Needs

- Proof of Concept ready
- Require resources to take MVP to market
- Seeking engineering support

Team from Queen's University Belfast

Dr Vishal Sharma
Principal Investigator and leading expert in drones & security

Prof. Trung Q. Duong
Co-Investigator and expert in drone, digital twin, and physical layer security

Dr Antonino Masaracchia
Researcher with experience in drone enabled networks

Contact details

Email: v.sharma@qub.ac.uk
Phone: +44 (0)28 9097 6813

IoTrim

Making IoT device connections secure with privacy-preserving AI

Market Need

The security and privacy of IoT devices is hard to control, making them vulnerable to attackers and malware. With 636 million people worldwide using IoTs in their home, the risk is palpable, as the team behind IoTrim discovered after substantial research.

Through extensive testing and research, the team found that the tools available right now simply don't work as they should. Many are unreliable, don't notify users of threats, can slow down the internet connection or even pose further risk from third-party services.

Solution

The team wanted to create a tool which anyone can use without needing specialist expertise. They created IoTrim to help monitor and block non-essential network activities, as well as identify device exposure and security threats, in an easy-to-use, 'plug and play' system.

Using privacy-preserving AI techniques, IoTrim builds insights and behavioural models, preventing violations of privacy by intercepting and blocking information exposure to third-party analytics and service providers. The solution uses unique methodology and can be built into the router itself.

Target Market

- Internet service providers (ISPs)
- Router manufacturers
- VPN providers

Status & Needs

- In contact with majors ISPs
- Phase 2 will see PoC feasibility study
- Seeking production expertise to optimise software

Team from Imperial College London

Dr. Anna Maria Mandalari
Co-Founder & CTO

Prof. Hamed Haddadi
Co-Founder & CEO

Dr. Daniel Dubois - Co-Founder

Prof. David Choffnes - Co-Founder

Vadim Safronov - Developer

Contact details

Email: anna-maria.mandalari@imperial.ac.uk

Website: iotrim.github.io

Twitter: @iotrim

Get involved in CyberASAP

Academics

CyberASAP welcomes participation from academics based all around the UK who have an interest in commercialising their cyber research. The programme is particularly keen to invite applications from academics in under-represented groups.

It is anticipated that a further CyberASAP competition, covering both Open and Thematic elements, will take place later in 2023.

Details will be posted at cyberasap.co.uk and via our social media channels. If you are interested in applying, please register your interest at cyberasap.co.uk (via the Get Involved section).

Cyber Security Academic Startup Accelerator Programme 22/23
To find out more about the programme and how to engage with it, visit cyberasap.co.uk

Mentors

Investors and industry colleagues with an interest in supporting the programme in any way are invited to provide their details via the Get Involved section at cyberasap.co.uk. We're always looking to extend our network of independent experts who provide such valuable input to the teams and enjoy insights into the cyber innovations being developed on the programme.

Thank You To All Our Mentors & Collaborators

CyberASAP is a collaborative enterprise, drawing on the experience and knowledge of Innovate UK KTN's Programme Directors, Emma Fadlon and Robin Kennedy, and their expert connections. This extended network of industry specialists who generously lend their expertise and insight to the academic teams is central to the success and impact of CyberASAP.

A huge thank you to each and every one of you.

Contact us

CYBER + ASAP | Academic Startup Accelerator Programme

Website: cyberasap.co.uk

Twitter: @CyberASAP

Email: cyberasap@iuk.ktn-uk.org

LinkedIn: /cyberasap

UKRI Innovate UK

UKRI Innovate UK KTN

Website: ktn-uk.org

Twitter: @KTNUK