CyberASAP Project Descriptions

Bournemouth University - Authentibility Pass

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

People with disabilities can encounter barriers due to web security and privacy technologies. This could result in them being prevented from purchasing goods or registering for services, leading to frustration and cancelling transactions. Authentibility Pass will be an innovative solution to assist people with disabilities, accounting for 15% of worldwide population and 14 million people in the United Kingdom, to communicate their authentication and accessibility requirements to higher education institutions, non-profit organisations, small medium enterprises and financial institutions. Our market validation highlighted that people with disabilities often need to repeatedly inform organisations of their authentication and accessibility requirements. Authentibility Pass will enable customers to enter their requirements into a smartphone application, which can be stored in secure organisational databases. The project will develop the Authentibility Pass Proof of Concept, consisting of an Android application, database and web interface for managing the database. The project team consists of academics from the Faculty of Science & Technology at Bournemouth University and Vers Creative UK will be sub-contracted to develop the Proof of Concept. Adopting Authentibility Pass will assist organisations to comply with accessibility and equality regulations, as well as facilitating awareness of the requirements of customers with disabilities when interacting with organisations.

University of Bristol – Surface RF

A Tamper Guard and Intrusion Monitor using Zenneck Electromagnetic Surface-waves. Making surfaces that identify, verify and protect themselves.

SurfaceRF is a spin-out from the University of Bristol specialising in making tamper detecting enclosures. Our technology determines the unique physical fingerprint of a surface using a patented form of 2-dimensional radar which travels only over the enclosure surface. This is monitored digitally and contact, modification or damage to that surface changes the fingerprint and triggers an alert. Due to the unique signature replacement of the protected system with a counterfeit will be detected. Items protected by SurfaceRF technology are made physically and digitally verifiable. The technology can monitor protected items actively or passively, depending on the desired application.

Our current proof of concept is lab based and in Phase 2 of CyberASAP we will build a portable demonstration unit and a number of reconfigurable prototyping kits we can use with end users to gain input and feedback for the final product. We anticipate being able to provide a product that is an extra layer of covert security capable of pinpointing when an unwanted physical intrusion has taken place. For example, a microdata centre in a hospital or finance office may be venerable to physical access. Our system can identify of any attempt to access the hardware containing confidential information.”

CYBER + ASAP | Academic Startup Accelerator Programme

Edinburgh Napier University – Memcrypt

Memcrypt protects and recovers confidential data from ransomware attacks.

Ransomware is a form of malicious software designed to block user access to files by encryption until a sum of money is paid. It is a growing global problem with estimated costs of $169 billion in 2020. Even without paying a ransom, costs include lost business, recovery time, third-party remediation services, and reputational loss.

Existing methods for combating ransomware include data backups, end-point protection, and cyber insurance solutions offered by third parties. However, these methods do not enable the user to quickly recover from an attack, when ransomware has succeeded in starting to encrypt user data. Memcrypt's core innovation will discover active ransomware keys and related artefacts and enable almost immediate data recovery.

For the PoC, we will develop a prototype named Memcrypt Triage which provides an out-of-the-box ransomware triage tool for incident response. The tool can be used to scan a target which has been affected by ransomware and will collect information of files affected by a ransomware attack. Our PoC will aid law enforcement in the collection of digital forensic evidence. The PoC will also help us better understand the characteristics of ransomware thus aid the development of our technology in ransomware key detection and data recovery.

University of Essex - SenseiChain

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

The blockchain market is showing a CAGR of 80.2%, with more and more businesses highlighting privacy concerns in blockchains. Permissioned blockchain provides integrity, immutability and transparency; however, lack of confidentiality is preventing enterprises from using blockchains to store sensitive data. Encryption of the blockchain data provides confidentiality but gives rise to lack of transparency, slow operations and inability to perform analytics on the data. Enterprises require an analytics capability on encrypted blockchain transactions, that ensures transparency and privacy of blockchain data.

SenseiChain is a highly secure patent pending technology that provides Secure Blockchain Analytics as a Service (SBAaaS), enabling the monitoring and analytics of encrypted blockchain transactions in real-time. SenseiChain provides enterprises with complete control and trust on the permissioned blockchain network, while generating real-time alerts on the analysed encrypted mission critical data. In comparison to its competitors SenseiChain offers both revolutionary analytics capabilities over encrypted blockchain transactions and superior levels of scalability; to provide improved security and privacy, reduced network latency and enhanced efficiency. SenseiChain technology is currently being patented and will benefit different verticals including defence organizations, law enforcement agencies, banking sector, IoT, healthcare domains and ecommerce sectors.

CYBER + ASAP | Academic Startup Accelerator Programme

Imperial College London – Shoji: Privacy-preserving Machine Learning as a Service

Unrivalled value from sensitive data silos with mathematically guaranteed privacy.

Shoji equips businesses with privacy enhancing technologies, helping them to safely maximise value from sensitive data assets.

Developed by a team of statistical machine learning researchers at Imperial College London, their privacy-preserving platform enables the joint analysis of distributed datasets belonging to multiple parties. For each party, their data remains securely on-premises, while differential privacy mathematically guarantees personally identifying information is never exposed. This empowers companies to safely overcome the obstacles preventing them from forming data partnerships, ensuring full regulatory compliance. Data silos can be broken down, allowing controlled access to vast amounts of data previously assumed to be inaccessible or impossible to share. Unlocking the value of this untapped data with private machine learning creates an opportunity for companies to innovate ahead of competitors while protecting customer data to build trust. For some, augmenting and enriching existing data unlocks new possibilities for data-driven decision making and actionable insight discovery. For others, licensing the private use of their data creates new revenue streams and freedom to collaborate.

Built by data scientists, for data scientists. Integration into existing ecosystems is seamless, making it easy and convenient to secure data in-use and place privacy at the forefront of data science operations.

Imperial College London - WhatML: Watermarking Machine Learning Models

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

Training machine learning models requires significant investments in the computing infrastructure, in acquiring and processing of huge amounts of data, and in the skills required to train the models to a high degree of performance. As a result, these machine learning models are hugely valuable assets that need to be protected. In many cases, these models are exposed, as they need to be deployed in the customer's facilities or in the final product. Other business models rely on outsourcing the training tasks to external suppliers or the use of marketplaces to buy and sell models specific to a task. All these forms of monetisation cannot be used without adequately protecting the models against theft, illegal copying and use beyond contractual terms. To address these shortcomings, we propose WhatML, a solution to protect the intellectual property of machine learning models through watermarking, enabling to verify the models' ownership or provenance. WhatML introduces watermarks in the model without impacting the system's performance; the watermarks are resistant to different model transformations. WhatML includes mechanisms to verify the model's provenance. It provides a novel and innovative solution. At the moment, there are no commercial products to protect the intellectual property of machine learning models.

CYBER + ASAP | Academic Startup Accelerator Programme

University of Kent - #ID Security for IoT

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

IoT devices are becoming ubiquitous with early applications ranging from smart-meters in the home through industrial control systems in factories to automated cars. The market potential for such systems is very high. However, this risk of compromise to the security of such systems makes them highly vulnerable, as existing security systems are inadequate for such applications. The primary aim of this proposal is to develop a proof of concept demonstrator of our #ID technology, demonstrating how it may be commercialised in the highly lucrative practical IoT environment where it demonstrates clear cost advantages over alternative techniques. The ability to provide a high performance protection system follows from its capacity to derive device identifying #ID's directly from the operating characteristics of IoT devices. This contrasts to the traditional approach where, for identification, a device either stores an identifier within it or typically submits a sample during a process called enrolment, and a digital representation of the sample is then stored as a template. Significantly, our proposed system does not store any templates or copies of the #ID's and therefore the opportunity for system breach via potential compromise is completely eliminated. This provides a disruptive technology with the capacity for enormous impact.

Lancaster University– Developer Security Essentials

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

Developer Security Essentials offers a cost-effective way to help any software development team improve the security and privacy of their code. It promotes cyber security and privacy as a business asset, makes them comprehensible to developers, and introduces the techniques needed to implement them correctly.

While a majority of UK software development teams still use at most one security technique, new laws mean that their organisations are penalised for security breaches, and cloud computing and DevOps mean that security must now be entirely in their code. Developer Security Essentials (https://securedevelopment.org/security-essentials/) provides a solution. It is a half-day package of structured workshops to motivate and empower developers to produce secure code, designed for non-specialist consultants and trainers to present.

In this project we shall develop proof of concept implementations of three aspects of the package: a version of the workshops that works effectively online, with professional usability, graphics and intellectual property constraints; a set of online questionnaires and the means to deliver them to assess the needs of a development team and the impact of the workshops; and a system for tracking referrals to other cybersecurity service providers.

CYBER + ASAP | Academic Startup Accelerator Programme

University of Leeds – Artificial Behaviour-Based Authentication for IoT (ABBA-IoT)

Data tampering detection system for automotive sensors.

"The aim of this project is to develop a proof of concept technology for an Intrusion Detection System (IDS) that monitors sensors on a vehicle for signs of cyber-attacks. Modern vehicles are equipped with hundreds of sensors that keep road users safe. Detecting attacks on them is a necessary step before any attack mitigation steps can be taken, it is also indispensable for forensics analysis to identify and mitigate vulnerabilities that cause a risk to road users. Our approach is built on an algorithm developed at the University of Leeds called “Artificial Behaviour Based Authentication” - ABBA. ABBA provides a mechanism to detect data tampering by generating a complex pattern in the communication network that would be disrupted by the actions of an attacker. This technology does not require prior training, handwritten rules, or a complex key management infrastructure the way its competition does. Instead, it is based on chaotic processes that are synchronised between devices to allow the detection of sensor spoofing or data injection on the vehicle’s network. This technique thus provides a practical advantage over alternatives. Additionally, ABBA is a “fully-on-board” system, meaning that vehicles would not require connection to a remote server to remain safe. "

Middlesex University – Linux

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

Linux is the predominant operating system for Internet Services and the National Critical Infrastructure. This makes these systems appealing targets for hackers. Unfortunately, Linux's built-in security access controls (SELinux and Apparmor) are underutilised due to their complexity. Additionally, the lack of support by third party security assessment tools for these systems makes them even more vulnerable to cyber-attacks. Therefore, we propose SALMAC, a unique security assessment tool for Linux system focusing on hardening SELinux and Apparmor in order to reduce the attack surface and to stop misconfiguration-based attacks in Linux environment.

Designed using a well-maintained threat model based on the MITRE ATT&K Framework, SALMAC gauges systems’ access controls against targeted attacks. And whilst simulating attacks, it pulls system logs from the targeted machines and links them to the launched attacks. This Event-Log pairing forms the basis for an effective threat hunting as well as being used to build the intelligence for an automated detection of future attacks.

SALMAC addresses the gap in the offerings of existing solutions and complements their features. We believe that with SALMAC, we play a role in supporting the NCSC's vision of "Making the UK the safest place to live and do business online".

CYBER + ASAP | Academic Startup Accelerator Programme

University of Plymouth – MaCRA (Software Tooling for Maritime Cyber Risk Assessment)

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

MaCRA (Maritime Cyber Risk Assessment) tooling will provide Dynamic Risk Assessment for the Maritime Sector, addressing a growing problem. This evidenced by high-value maritime cyber-attacks occurring on a weekly basis on shipping platforms with a complex mix of both IT and OT, in a system that often includes many legacy elements combined with increasing autonomy.

MaCRA is based on a publication in the journal of Maritime Affairs in 2019, and the framework generates a new risk profile for a specific operation if any parameter in the system is changed. This having advantages over static, sequential risk assessment frameworks which have very limited application for shipping. Crucially, this will look at; 1) the Ship's system, but then also 2) the cargo being carried, and then 3) what route the vessel is taking. And then by applying known issues for 2 and 3 against the vulnerabilities known for 1, we can then produce a more informed risk assessment for the vessel or fleet in question. We will look at both IT and OT aspects of the system too, so that profiles generated will inform operators exactly where mitigation efforts should be applied, taking in areas including technical fixes, and training.

University of Southampton – CyberHelper

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

Our society is facing an increase of 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 aggravates 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, knowledge representation, and decision making, to guide security analysts in the analysis of cyberattacks. CyberHelper works with different types of information and increases the efficiency of the investigation by providing the analyst with AI-driven insights and guidance, thus, reducing the investigation time.

CYBER + ASAP | Academic Startup Accelerator Programme

University of Strathclyde – Lupovis: A Wolf in Sheep's Clothing

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

Lupovis, a spin-out from the University of Strathclyde, provisions agile deception environments that enhance cyber protection frameworks. Lupovis' services and tools create active deception-based environments enabling early threat detection with attacker characterisation, informing on the most effective countermeasure to arrest insider threats, ransomwares and stolen credentials. Advance Machine Learning software manipulates attackers, luring their path away from the valuable assets whilst gathering information on the skills levels, resulting in enhanced operational (business) continuity for critical infrastructure organisations and a more granular incident response.

University of Wolverhampton – CyberMIND

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

CyberMIND is an AI-based platform helping Cybersecurity professionals to detect, predict and manage stress. Cyber professionals, like front line soldiers in a warzone, protect our organisations and critical infrastructure. But due to an increase in the number of sophisticated attacks, shortage of skilled staff and overwhelming workloads nearly 50% of them are suffering from mental health issues. So, how secure are we? CyberMIND, helps you predict and manage your cyber team's mental health and wellbeing. The result: improved performance, productivity and reduced cyber risk. As 40% of your team will leave by the end of the year, due to stress, what will this cost you? And remember you have a Duty of Care to assess stress so, are you looking after your cyber team? Would you like a solution with an ROI of just a few days? Let's connect. E.Kay@wlv.ac.uk