Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
PYTILIA LIMITED	Data Path Development Kit	£79,195	£55,436

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
This project will demonstrate the use of DSbD technologies in the field of IT infrastructure components. The specific application used in this project is a packet processing application but we believe the project's findings will be applicable to a broader range of infrastructure components. The project will explore the use of both pointer protection and memory compartmentalisation within the data path layer of a full stack application and particularly in a performance-sensitive context.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
OXON.TECH LTD	Porting Edge AI Workflows to CHERI/Morello	£77,706	£77,706

Project description - provided by applicants
Oxon Tech is currently finishing Phase 2 of a GovTech Catalyst funded project on behalf of Mid and West Wales Fire and Rescue Services to create an indoor tracking system, capable of being instantly deployed to incidents with no existing infrastructure requirements. A core component of our platform is a body worn edge IoT device that incorporates an IMU, an ARM process, ARM Microcontrollers and a Neural Processing Unit for running AI The platform also includes a visualisation system that gives incident commanders instant situational overview of where all of their assets are deployed as well as an instantly deployable secure wifi / 4g network. Although the Fire and Rescue Services are an excellent and highly worthy market for this product, commercially the military and law enforcement sectors are far more viable. Creating and securing a platform that spreads across body worn edge iot devices, to incident commander tablets, to cloud based control centers is a huge challenge, and the fact that it is potentially carrying data on troop or police deployment makes it an incredibly likely target for attack. Our main focus will be on porting as much of our existing stack to Morello FVP as possible, identifying and solving any dependency issues that arise. We will also carry out a thorough assessment of options for incorporating hardware devices including NPUs, by either USB passthrough to the FVP if possible or emulation. By the end of the project we aim to have created as much public documentation on porting IoT, ROS based and if time allows FreeBSD based systems as possible, as well as built up significant in-house expertise in DSbD technologies.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Participant organisation names	Project title	Proposed project costs	Proposed project grant
MINDHUG LTD	Multi Compartment Computation Protocol based on DSbD	£88,811	£79,930

Project description - provided by applicants
Through this project, we will contribute to our industry's understanding of how to build a Multi Compartment Computation protocol that provides distribution of a computation across multiple compartments where no individual compartment can see the other compartments data. As company, we require this for our products but the opportunity is much bigger than our sector alone (mental health records). Many use cases exist, for example in financial services, in enterprise and in media to enhance security around secrets, data and content. With this grant, our objective is to investigate a solution that could mitigate current vulnerabilities and challenges posed by physical Hardware Security Modules (HSMs), by researching a secure multi-compartment computation protocol framework to securely and privately compute on distributed data without exposing or moving it by controlling dataflows within object capabilities via isolated compartments with assured pipelines. We are a passionate Mental Wellbeing SME but security underpins our technology for MHR safety, our positioning and our growth. The work focuses on application layer compartmentalisation with modular abstracted compartments that can compute on its capabilities without ever exposing or moving it.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Participant organisation names	Project title	Proposed project costs	Proposed project grant
DRISQ LTD	CHERI Standards Compliance (CHERI Stone)	£60,315	£60,315

Project description - provided by applicants
The adoption of autonomous systems and the use of technologies for Industry 4.0 rest in part on the security and safety assurance of the underlying technologies. For most commercial processors, the development material is not widely available leading to defensive architectures that add significantly more cost and risk to such embedded systems programmes. The adoption of 'capabilities' would mean little to most developers and what it means for the potential use within embedded systems. The CHERI programme provides an opportunity to examine the available material in light of commonly used standards such as those used in the aerospace sector. The project seeks to understand what evidence from the CHERI project could be used to support compliance to internationally recognised standards such as DO-178C/ED-12C and DO-326A/ED-202A. We intend to write an open report on the implications of the new technology in embedded systems safety and security.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
IOETEC LIMITED	SecurIOT	£74,483	£74,483

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants
The DSbD challenge investigates projects that help UK digital computing infrastructure to become more secure. An area of concern that still requires further investigation is the security of devices connected to the main secured system, commonly referred to as the Internet of Things (IoT). With an estimated growth of up to 50 billion connected devices over the next few years and evidence that 98% of all IoT device traffic is unencrypted, exposing confidential and personal data on the network, there is a growing cybersecurity risk, which if left unaddressed will result in significant vulnerabilities. IoT has a complex set of security challenges, in particular that they are often resource constrained with limited power, processing and memory and are typically cost sensitive. Ioetec have developed a platform for securing IoT data and the aim of this project called SecurIOT, is to investigate the feasibility of incorporating DSbD hardware and software into IoT gateways to allow improved security of the connected sensor devices and their data. This poses significant technical and commercial challenges to see if a commercially viable solution can be achieved.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
VERIFOXX LTD.	A TEE-aware compartmentalization framework based on DSbD	£79,550	£79,550

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants

Through this project, we will contribute to our industry's understanding of how to build a capability architecture based Trusted Execution Environment (TEE) that provides strong isolation and secure data sharing across the secure and normal worlds. As a company, we require this for our products but the opportunity is much bigger than our sector alone (identity verification). Many use cases exist, for example in financial services, in enterprise and in media to enhance security around transactions, data and content.

With this grant, our objective is to investigate a solution that could mitigate current vulnerabilities posed by existing TEEs, by researching a capability architecture based TEE development framework for strong isolation and secure sharing of systems resources and application data across secure and normal worlds by controlling dataflows within object capabilities via isolated compartments with assured pipelines.

We are a passionate AIOT SME but security underpins our technology, our positioning and our growth. TEEs is an area our CTO has done a lot of work in. Winning this grant would allow us to put resource behind this real market problem. Our vision is that this research could be used as a basis for us to build a prototype in the future, which would strengthen not only our product's security, but also play our part in radicalising the UK's digital computing infrastructure.

Using the FVP platform with CHERI processor prototype, CheriBSD kernel, Clang/LLVM and CheriBSD's userspace, our key objectives are to:

* Investigate the performance, semantics, vulnerability mitigations and merits of compartmentalized TEE in comparison to existing standard TEE environments Intel SGX and ARM TrustZone TEE
* Understand if a framework like this helps towards ease of development and adoption as well as knowing if it supports hardware independence
* Explore enclave life cycle management

We will focus on the application layer compartmentalization by separation of concerns between the normal world and secure world functions, and further decomposition of capabilities within the secure (enclave) world including modular abstraction with isolated compartments with single responsibility principles and the separation of privileges.This is innovative because working with DSbD technologies, it aims to move the separation of concerns between the two worlds away from the hardware or the OS stack while retaining the integrity of TEE but addressing the vulnerabilities of existing approaches.

After completing this research, we endeavour to build a prototype framework for further testing internally, and ideally with the wider software and DSbD community.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Participant organisation names	Project title	Proposed project costs	Proposed project grant
ANZEN TECHNOLOGY SYSTEMS LIMITED	A feasibility study of a data security software product adopting Digital Security by Design (DSbD) technology	£76,706	£53,694

Project description - provided by applicants

The Anzen data archive and storage product is a software innovation that allows organisations to store their data in the public cloud with an increased level of assurance that it will not be leaked or compromised. It achieves this by data anonymisation via clustering, followed by splitting it into four separate data shards which may individually stored in different locations. This solution means that without compromising each of the four storage locations it is impossible to return the data to its original form and therefore massively multiplying the amount of effort required in order to compromise the data.

The key project objective is to confirm whether adopting DSbD security is viable. We therefore require to understand whether our product's functionality behaves the same and whether we have the requisite have the skills and resources that is both practical and achievable for DSbD technology adoption. The study deliverables therefore will be framed to answer this question through research and design of feasibility experiments; the execution/testing of these; and the analysis of both the quantitative and qualitative results.

Our investigation of the work required in order to move an existing piece of software (in this case our core processing code) will act as guide for other software projects and our own future works as to the viability of supporting CHERI.

The investigation will focus on determining the technical and knowledge challenges encountered when migrating an application in the middleware of the software stack. This investigation will evaluate not only the CHERI architecture itself but also the supporting documentation, operating system support and the LLVM/clang compiler for CHERI.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Note: These proposals have succeeded in the assessment stage of this competition. All are subject to grant offer and conditions being met.

Participant organisation names	Project title	Proposed project costs	Proposed project grant
METRARC LIMITED	Trusted Ring Security for Mortello Devices	£39,964	£27,975

Note: you can see all Innovate UK-funded projects here: https://www.gov.uk/government/publications/innovate-uk-funded-projects
Use the Competition Code given above to search for this competition's results

Project description - provided by applicants

This project will develop Metrarc's Trusted Ring cybersecurity technology implementation for the DSbD Mortello platform, to both evaluate the full stack design process as part of the project and investigate the suitability of this platform to further enhance the degree of security provided by the Trusted Ring technology. The Trusted Ring approach facilitates to establish trust and provenance in the identity and integrity of digital devices via their inherent physical and behavioural characteristics by creating a group of interacting devices that are linked in a secure manner thus establishing the Trusted Ring. This Trusted Ring is an additional security layer which enhances incumbent security systems that Metrarc has developed thus far and is so far targeted on traditional digital systems and IoT devices.

This project will address the holistic issue of security when connecting multiple devices and services utilising communication infrastructure. The proposed system will solve issues related to the trust and providence of the communication infrastructure / device interface, a lack of confidence in which may inhibit full utilisation of low resource digital devices and prevent the spoofing of such devices compromising users' confidential data. As the adoption of digital technologies expands, it becomes vital to build trust and confidence in the integrity of such technology. Metrarc has developed a novel technology for deriving encryption keys directly from the operating characteristics of digital systems, a unique and patent protected technology termed ICMetrics. This proposal will significantly enhance this already secure technology by allowing the range of devices participating in any interaction to vary, whilst still ensuring that it builds upon the security features of existing, practically employed systems and can integrate the new DSbD Mortello platform. The project will investigate the major case study area of connecting Mortello based digital devices to communication infrastructure and further integrate the verification process of a range of services which may be accessed via the communication infrastructure. The projects therefore aims to establish mutual trust between the devices, communication infrastructure and connected services via the Trusted Ring architecture.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Participant organisation names	Project title	Proposed project costs	Proposed project grant
VALID DATUM LIMITED	Quantum Resistant DSbD Security Leveraging MicroTokenisation	£79,726	£79,726

Project description - provided by applicants

ValidDatum Limited, rapidly-growing UK-based cybersecurity and data protection service provider, Value-Added Reseller of Eclypses MTE technologies, and software solutions developer with an emphasis on data pseudonymisation and tokenisation for guarding against mass data breaches. Ms Daryl Crockett, CEO, serial software entrepreneur and leader in data security integration, privacy-by-design, and data management in business digital transformations. Ms Chris Morecroft, UK Managing Partner, brings significant compliance experience as a fraud examiner, advisor, and data security and privacy director. Mr Tee Patel, CISO, is a noted cybersecurity architect, and frequent keynote speaker.

Vision

ValidDatum is of the mindset that business and operational digital ecosystems are complex and dynamic. Whenever possible, data should be protected through the use of pseudonymisation and tokenisation. Present-day data security practise relies on intrusion detection, ring-fence defences, and cumbersome encryption key management. But, if these defences are circumvented, bad actors can access our most private and precious data, exposing individuals, companies, and governments to catastrophic data breaches. Recent events have demonstrated that there are abundant ripe entry point targets for bad actors in our modern business systems, where those with malicious intent can use their continuously evolving collection of tools to gain access to data such as phishing, trojans, code injection, password attacks, eavesdropping, and now, on our doorstep -- nation-state Quantum computing attacks and encryption chaining pattern detection. We must work collaboratively and tirelessly to develop security applications and ecosystems to thwart these attacks; bearing in mind this core principle -- that when the data we seek to protect is readable, it is vulnerable.

Key Objectives & Focus

ValidDatum seeks to support the growth and fortitude of the Digital Security by Design Software Ecosystem through the investigation of the feasibility of its existing technologies for:

1.) Integrated synchronous encryption key management technology within libraries, automatically generating unique encryption keys for individual pieces of data to reduce the risk and overhead of traditional encryption key management.

2.) The employment of End-to-End Payload Protection for data-in-transit, providing an uninterrupted layer of protection for data on its journey within the ecosystem.

3.) The usage of Android device jailbreak detection to reduce the risk of malicious entry-point exposure and data-interception through mobile device applications.

Results of Competition: Development of the Digital Security by Design Software Ecosystem

Competition Code: 2011_ISCF_DSBD_FULLSTAGE

Total available funding is £1.5m

Participant organisation names	Project title	Proposed project costs	Proposed project grant
CAPABILITIES LIMITED	Assessing the Viability of an Open Source DSbD Desktop Software Ecosystem	£54,000	£54,000

Project description - provided by applicants
This project is assessing the applicability and viability of DSbD technologies to a complete open-source desktop environment software stack. Through a blend of static and dynamic analysis, as well as prototyping, we will identify opportunities to deploy CHERI memory protection and software compartmentalization within software components such as window systems, desktop toolkits and environments, as well as key applications such as web browsers. We will assess the potential cost, complexity, and overheads associated with CHERI deployment in those software environments, and make recommendations for future work to deploy CHERI protection within these open-source stacks.