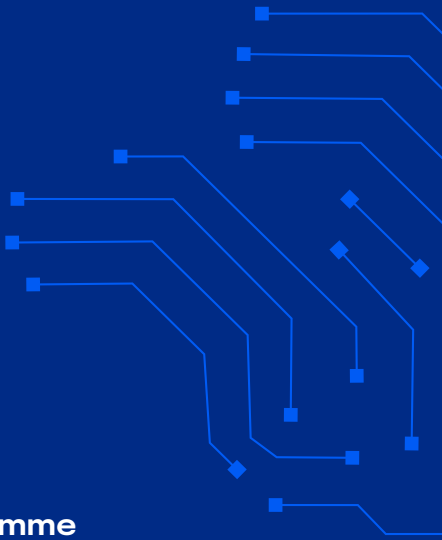
Digital Security by Design



Technology Access Programme

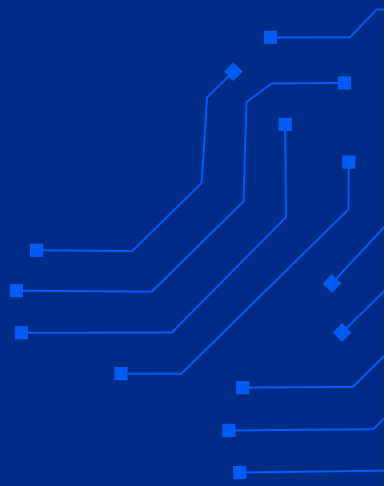
Demo Day

22 March 2023
Hosted by Digital Catapult

UK Research and Innovation

CATAPULT Digital

Website	dsbd.tech
LinkedIn	/digital-security-by-design
Twitter	@dsbdtech
YouTube	@digitalsecuritybydesign



Digital Security by Design

Transforming technology to create a more resilient and secure foundation for a safer digital future.

Digital Security by Design (DSbD) is an initiative supported by a consortium of leading technology companies, academic institutions, researchers, and UK government agencies. As well as enabling a more trustworthy digital environment, DSbD is driving a mindset change around cyber security.

The DSbD Technology Access Programme Demo Day is a showcase event that celebrates a year of experimentation. Each participating company has tested innovative prototype technology from Arm and the University of Cambridge, and is sharing their experiences of how it could work in the real world. By demonstrating its potential and capabilities (as well as discussing any practical challenges), our collective aim is to inspire other organisations to take up the technology once it becomes commercially available.

Introduction

John Goodacre
UKRI, DSbD Challenge Director

Our digital world continues to grow exponentially, providing opportunities that previous generations could only dream of. However, with those opportunities we are also opening up new ways for cyber criminals and bad actors to exploit the fundamentally insecure foundations of our computing infrastructure.

The Digital Security by Design (DSbD) programme is seeking to fix those foundations by realising technical developments at a scale computing has not seen for 50 years. These developments are anticipated to block exploitation of around 70% of ongoing vulnerabilities, while providing software developers with new ways to keep us safe. To achieve this goal, DSbD has been engaging with government, industry, and academia to ensure that this new approach is proven, has a supportive ecosystem, and can show real-world security and resilience benefits.

Through the DSbD Technology Access Programme (TAP), Digital Catapult has been integral to ensuring that UK businesses can review and understand the new technology involved, while preparing for its adoption in their future products or services. An ecosystem of companies is now ready to take full advantage of the cutting-edge technology once it becomes commercially available.

Since the inception of DSbD in 2019, individuals and organisations have been showcasing benefits of the technology far beyond those originally conceived at the outset. DSbD is building a solid evidence base that the 'secure by design' approach has a significant impact on building a more resilient and productive digital future, and the UK Government is embedding DSbD into national security strategies and agendas.

By fixing our computing infrastructure, we can achieve the scale of change necessary to make the world of computing more secure, and ensure a safer future for all.

“

Digital Catapult works with companies using advanced digital technologies to achieve their own individual goals. This time, the goal is shared, and it’s exciting to be progressing the early development of a game-changing cyber security technology. Working alongside deep tech companies, we’re learning together as we help to advance use cases and provide valuable feedback for the wider DSbD ecosystem.

TAP is a powerful example of technology development in action, and it’s great to be showcasing the results so far. The DSbD technologies have huge potential to make a difference for all kinds of industries, and the aspiration is that this approach to cyber security will become a standard for the future. Today’s event is a milestone in the ongoing journey, as we continue to support UKRI in achieving that aim.

Jessica Rushworth
Chief Strategy & Policy Officer, Digital Catapult

Technology Access Programme

Delivered by Digital Catapult, the DSbD Technology Access Programme (TAP) gives UK-based companies access to a Morello board, CHERI (Capability Hardware Enhanced RISC Instructions) stack, and technical support for trialling a new approach to cyber security within their systems, products, and applications.

TAP participants benefit from one-to-one guidance and ongoing support from Digital Catapult’s and University of Cambridge deep tech experts. Information and findings are constantly being shared within the connected TAP community, with regular facilitated meetings and discussions also taking place.

Developed by Arm, the Morello evaluation board is a test platform for the Morello prototype architecture, based on the CHERI protection model. CHERI is a novel extended instruction-set architecture developed by the University of Cambridge and SRI International.

This cutting-edge technology is capable of preventing around two thirds of hacks, cyber attacks and data breaches. It can defend against most known memory safety issues in C and C++, and can be used to uncover security vulnerabilities in systems. One of the significant advantages it offers is the ability to upgrade the security posture of legacy systems without having to move to a new programming language.

Introducing the Arm Morello board

Richard Grisenthwaite,
Executive Vice President and Chief Architect, Arm

Securing the world's data will be one of the greatest technology challenges over the next decade of compute. If the Morello prototype architecture performs and can be widely used as expected, it will be fundamental in future processor designs, protecting businesses, individuals and the devices of tomorrow.

What is the Morello program?
The Morello program is a research program led by Arm to create a more secure hardware architecture for processors of the future. Its unique architectural extensions are based on Arm's work with the University of Cambridge since 2015 on the CHERI (Capability Hardware Enhanced RISC Instructions) protection model. CHERI architectural extensions are designed to mitigate memory safety vulnerabilities – software defects that are exploited by hackers to take control of a device or system – at a hardware level.

The Morello program aims to assess the viability of the Morello Board, a prototype hardware system on chip (SoC) employing unique extensions to the conventional Arm hardware instruction set that significantly improve device security.

What's the latest on the Arm Morello program?
Over a year has passed since the Morello program celebrated the first availability of prototype SoCs (systems on chips) in January 2022. The limited-edition Morello boards are based on the Morello prototype architecture embedded into an Armv8.2-A processor (an adaptation of the Arm Neoverse N1 processor). Over 500 Morello boards have now been distributed to our ecosystem of security specialists, software companies, tools developers, leading academic institutions and participants of the DSbD Technology Access Programme. Researchers and developers are now able to test, write code and collaboratively provide critical feedback to identify whether Morello is a viable security architecture for the future.

CHERI: from research to reality

Professor Robert N. M. Watson, Department of Computer Science and Technology, University of Cambridge

Since Simon W. Moore (University of Cambridge), Peter G. Neuman (SRI International), and I began work on developing CHERI in 2010, the possibility of a highly disruptive hardware change to radically improve security has gone from blue sky thinking to practical reality.

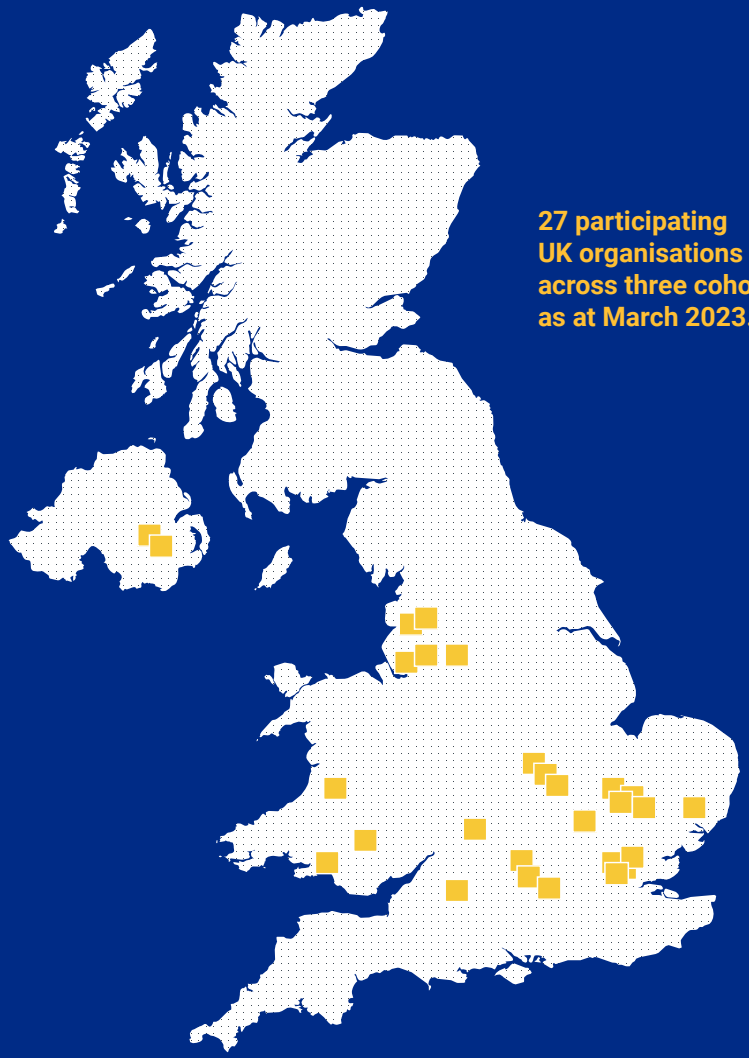
DSbD has been an essential part of this realisation, creating the first industrial-quality demonstrator of the CHERI concept, Arm's Morello prototype processor, SoC, and board. This has resoundingly validated a key hypothesis regarding the viability of the hardware approach.

Another essential hypothesis for CHERI has been the ease with which it can be adopted in software, which TAP has played a key part in validating.

We are immensely proud of the work being undertaken, enabling dozens of companies and universities around the UK to engage directly with the Morello prototype and explore its impact on their own diverse products and systems.

The results have been highly satisfactory: TAP participants have met with us regularly throughout the programme, initially to learn about CHERI, and later to offer us detailed feedback on improving the technology and its delivery.

During the programme, we have been introducing new uses of CHERI in software, including spatial safety and new software compartmentalisation features. We look forward to continuing and extending this exciting collaboration with future TAP cohorts.



27 participating UK organisations across three cohorts, as at March 2023.

Programme scale so far

+ 12 million lines of code ported to Morello by Cohort 1 and 2

+ 1,250 working days invested

14 networking and learning events

Multi-sector and cross-discipline involvement

including cloud computing, consulting, telecoms, IoT, software development, IT services, utilities, automotive, manufacturing and defence

Get Serious about SaaS – understand the risks and rewards of adopting cloud-hosted applications

Location	Belfast
Email	info@ampliphae.com
Website	ampliphae.com
LinkedIn	/ampliphae-ltd
Twitter	@Ampliphae

Ampliphae

Scope of project

SaaSGuard is Ampliphae's security and regtech product, helping their global clients to manage risk and maintain compliance as they adopt cloud applications. SaaSGuard appliances (x86-based) are deployed across the customer infrastructure and collect data into SaaSGuard Cloud for analysis of SaaS adoption. The Ampliphae team has been experimenting with CHERI and the Morello board to assess its value as a secure stack for SaaSGuard IoT appliances, and to understand the trade-offs versus their x86 platform.

Results

The project has enabled their team to engage with CHERI/ Morello and the flourishing ecosystem of cohort companies and affiliated contributors, and initial experimentation with the board has been encouraging. They continue to evaluate the potential for a CHERI/Morello-based IoT network appliance, with a focus on secure post-quantum communications and high line-rate (10Gbps+) applications.

Chevin Technology

Chevin delivers high performance, configurable Ethernet IP cores for FPGAs. Chevin's goal is to provide reliable, hardware accelerator capabilities for high end FPGAs that are cost-effective and straightforward to implement, while using minimal FPGA resources.

Location	Cambridge
Email	info@chevintechnology.com
Website	chevintechnology.com
LinkedIn	/chevin-chevin-technology
Twitter	@TechChevin

Scope of project

Chevin has a unique method for managing licences in a system with two nodes, a licence server and one or more licence clients (patent pending).

Their project aims to establish communications over TCP (Transmission Control Protocol) between the client and server, with the TCP being used to carry out licence authentication and authorisation, using messages passed between the nodes.

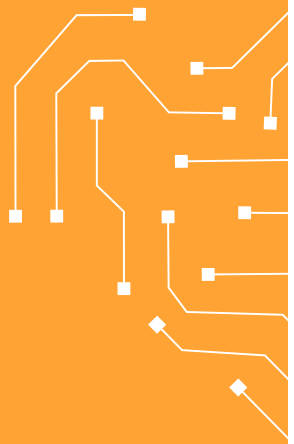
Results

After setting up Morello and building CheriBSD, the team has been able to compile and run code, and successfully port and run their TCP client/server application on Morello.

Ioetec

Ioetec specialises in security for the internet of things to provide confidentiality, integrity, and authenticity of data.

Location	Sheffield
Email	sales@ioetec.com
Website	ioetec.com
LinkedIn	/ioetec
Twitter	@totallysecure



Scope of project

Ioetec has developed a full stack software solution to secure internet of things (IoT) devices. This ensures that the data is secure in transit and at rest from the sensors where the data is generated, through to the user where it is consumed. Ioetec's project has focused on attempting to use the Morello hardware as a gateway solution for IoT.

Results

This project has enabled their team to engage with CHERI / Morello and the flourishing ecosystem of cohort companies and affiliated contributors. Their initial experimentation with the board has been encouraging. The team intends to continue evaluating the potential for a CHERI / Morello based IoT network appliance, with a focus on secure post-quantum communications and high line-rate (10Gbps+) applications.

RealVNC

RealVNC's secure remote access is used every day by millions of people worldwide.

Location	Cambridge
Email	enquiries@realvnc.com
Website	realvnc.com
LinkedIn	/realvnc
Twitter	@RealVNC

Scope of project

RealVNC's aim was to port their Connect remote access software to CheriBSD, with all applications and their dependent libraries running in pure capability mode. Compiling, running, and testing their software on the Morello platform allows the RealVNC team to immediately spot the types of programming errors that may have the potential to affect security.

Results

Their Connect software is fully ported to CheriBSD on Morello hardware, with the CHERI ABI/ pure capability mode enabled. This allows the benefits of CHERI to be applied to remote access use-cases, either as a secure client, or desktop, or both.

RealVNC has analysed protection faults (provoked intentionally and otherwise) and used the findings to expand their understanding of these types of vulnerabilities.

Riskoa

Riskoa is a engineering technology company providing digital solutions for water management, assessment and remote monitoring.

Location	Preston
Email	info@riskoa.com
Website	riskoa.com
LinkedIn	/riskoa

Scope of project

Watsion Clarity is Riskoa's product for remote water quality monitoring. The battery-powered hardware unit connects to a water stream in a district-metered area within a water utility network, takes a water sample, and passes it through a series of Modbus water sensors. It then sends the data to an IoT platform.

The security of feedback sensors is becoming ever more important to customers in the water sector, which is why Riskoa's product scope was to look at ways of enhancing Watsion Clarity's security offering.

Results

Riskoa's product architecture has been successfully deployed on the Morello board and CHERI application. The main development for the Riskoa team was deployment of a Modbus library for Morello applications.

Sensor IT

Sensor IT is a UK-based internet of things technology provider and manufacturer.

Location	London
Email	info@sensorit.co.uk
Website	Sensorit.co.uk
LinkedIn	/sensor-it-uk

Scope of project

Sensor IT ported a complete application suite as part of their participation in the DSbD programme. The application, a complete SMTP+POP3+IMAP4 package, symbolises the most critical layer of systems exposed to potential hacking attempts, as it is constantly accessed by third parties. The Sensor IT team was aware of existing vulnerabilities in the package, and intended to use the new hardware/ software platform to validate its security capabilities.

Results

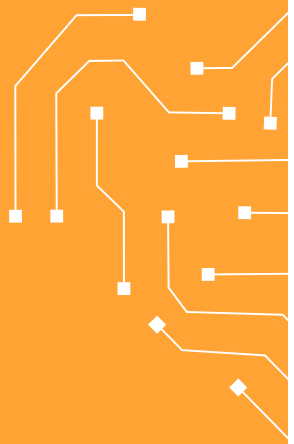
During the porting exercise, the suite was subjected to external attacks and exploit packages that demonstrated the security credentials that the Morello board and CheriBSD offered.

Sensor IT validated this by using the Morello board/CheriBSD; vulnerabilities that initially existed in the software suite were patched up and no root access was allowed by exploiting memory overflows.

Telkoa

Telkoa supports telcos and IoT providers with actionable insights, to help them reduce costs, increase ARPU and enable new services.

Location	Preston
Email	hello@telkoa.com
Website	telkoa.com
LinkedIn	/telkoa
Twitter	@Telkoa_Techs



Scope of project

Deploying a license server on-premise where the customer doesn't permit internet connectivity is challenging. Telkoa's DSbD project uses Morello and CHERI to secure sensitive information on-premise.

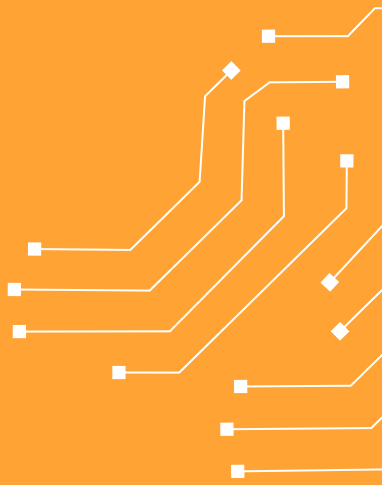
Results

Telkoa has built the license server application on the Morello board using CheriBSD. The project team has found that this setup makes it challenging for an attacker to gain access to secured information, and tests have shown that simulated attacks are being defended against.

3bian

3bian is a software development company specialising in power-efficient computing.

Location	Birmingham
Email	dsbd@3bian.co.uk
Website	3bian.co.uk



Scope of project

The 3bian project scope was to create a functional Linux image and obtain a deeper understanding of how to convert programs to run on the Morello platform.

Results

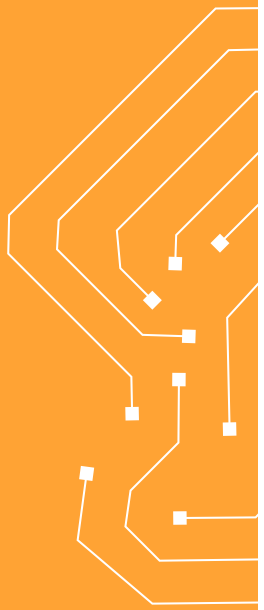
3bian created several veneers to mediate between the traditional AARch64 and Morello worlds. As the team modified programs for Morello, they started to see patterns emerging. They then created tools for finding these patterns in other source code.

During development, 3bian also created a Debian repository for pure-capable software.

Nick Connolly

Building SPDK & DPDK to run on CheriBSD & Morello

LinkedIn /nick-connolly-36276339



Scope of project

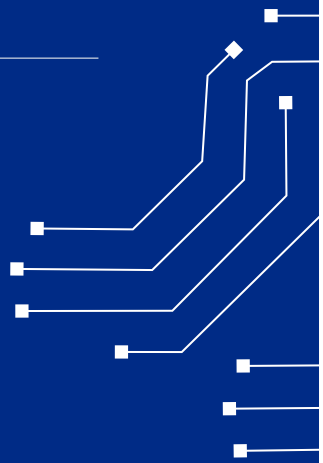
Nick started the project working at DataCore, but has since left the organisation. His project scope was to construct a CHERI-enabled user space storage stack using the open source Storage Performance Development Kit (SPDK) that demonstrates secured-by-design access to highly performant persistent data on locally attached storage. The project also included work on the Data Plan Development Kit (DPDK).

Results

Nick has been able to set up Morello and built CheriBSD in purecap mode. He has built DPDK and run basic tests, followed by DPDK contiguous memory driver. He has built and deployed a DPDK kernel module and has built DPDK dependencies in pure-cap mode and has also built SPDK in pure-cap mode too.

Part of Capgemini Invent, Cambridge Consultants delivers breakthrough innovation to transform business and change the world.

Location	Cambridge
Email	defence@cambridgeconsultants.com
Website	cambridgeconsultants.com
LinkedIn	/cambridge-consultants
Twitter	@CambConsultants



Cambridge Consultants

cambridge consultants
Part of Capgemini Invent

Scope of project

Cambridge Consultants set out to determine the extent to which CHERI could help develop more secure technologies for their clients. The project aim was to assess the capability and maturity of the Morello platform for delivering enhanced security for the systems they create. This would involve porting some existing code and evaluating the ease of porting and the performance and security of the resulting system.

Results

Initial platform setup was a longer and far more involved process than anticipated. Cambridge Consultants also found that there was a steep learning curve for effective use of CHERI capabilities. They were able to overcome these issues and successfully ported an existing implementation of an LTE mobile base station stack, which they will use to explore the level of security benefits CHERI offers.

CAN-PHANTOM

CAN-PHANTOM is a UK manufacturer of advanced vehicle immobilisers. The company's aim is to secure as many vehicles as possible to end the rising surge in vehicle theft.

Location	Stafford
Email	enquiries@can-phantom.com
Website	can-phantom.com
LinkedIn	/canphantomlimited
Twitter	@can_phantom

Scope of project

The project scope for CAN-PHANTOM was evaluation of the technology for use in low-level embedded IoT telematics applications, with the Morello board acting as the main controller for a CAN-based vehicle immobiliser with built-in vehicle tracker. The company is testing the viability of this technology for use in aftermarket automotive devices, and has successfully experimented with GNSS and mobile technologies.

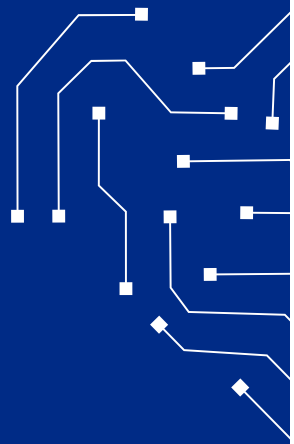
Results

Currently, CheriBSD doesn't support CAN devices, so the team has started work on supporting USB-to-CAN devices using libusb and working with the CheriBSD developers to fix any issues encountered. So far, the technology has helped them find errors earlier than normal, although it can also cause some subtle (but well-documented) errors.

Cedyr Labs

Cedyr specialises in batteries and smart power electronics, enabling enterprise customers to intelligently design, monitor, manage and optimise their fleets of electric-powered assets.

Location	Manchester
Email	hello@cedyr.com
Website	cedyr.com
LinkedIn	/cedyrlabs
Twitter	@CedyrLabs



Scope of project

Cedyr's project is based on the libiec61850 library, an open-source (GPLv3) implementation of the IEC61850 protocol stack that has been successfully used in several commercial software products and services.
Cedyr has successfully ported the libiec61850 library with CHERI capabilities on the Morello platform. To assess the ported library's functional, security, and performance benefits, the team then created a testbed simulating the IEC61850-based smart substation.

Results

Results have shown that the ported library could successfully perform operations related to data sets and reporting. For in-depth vulnerability discovery, the Cedyr team performed fuzzing tests using the LLVM's LibFuzzer module. They also performed elementary performance tests to assess the benefits of the ported library.

DONAA

DONAA detects defects in 3D printing in real-time, enabling users to cut costs and protect the environment.

Location	Coventry
Website	donaa.ai
LinkedIn	/donaa
Twitter	@DONAA3Dprinting

Scope of project

DONAA's project involves using video analysis to detect defects on recorded high value 3D printing processes, and sending notifications as defects occur. The aim is to deploy some of DONAA's algorithms on the new CHERI/Morello solution, assess performance, and compare it with standard architectures. The performance metrics include speed of processing and safety.

Results

No noticeable differences in the processing speed were observed during initial tests, so real-time processing with at least comparable performance between CHERI/Morello and standard architectures is expected. Early results from threat modelling suggest that considerable improvements can be achieved. These include securing access to sensitive data, and preventing data corruption related to defect detection.

Dynamic Devices provides a range of embedded and internet of things integration services, supporting clients through concept, prototype manufacture, platform integration, scale-up, volume manufacturing and post-sale platform support.

Location	Liverpool
Email	info@dynamicdevices.co.uk
Website	dynamicdevices.co.uk
LinkedIn	/alexjlennon
Twitter	@embedded_iot

Dynamic Devices

dynamic devices LTD

Scope of project

This project is focused on bringing Yocto embedded Linux support for Morello/CHERI to a global embedded ecosystem.

Results

The Dynamic Devices team has engaged with collaborators on Yocto development, including Arm and The Good Penguin, and have successfully booted a CHERI-enabled Yocto Poky operating system on the Morello platform.

KATLAS addresses secure, scaleable, and shareable multi-vendor interoperability for automated systems.

Location	London
Email	edward.cole@katlastechnology.io
Website	katlastechnology.com
LinkedIn	/katlastechnology

KATLAS

KATLAS
Accelerating innovation

Scope of project

The KATLAS DSbD project studies available compartmentalisation models protecting against future software bugs that could compromise a user's private data. The focus of this study is on finding the smallest and most elegant change to the KATLAS legacy codebase that would enable effective protection against leakage for its software design pattern, where the address space contains multiple privacy wallets.

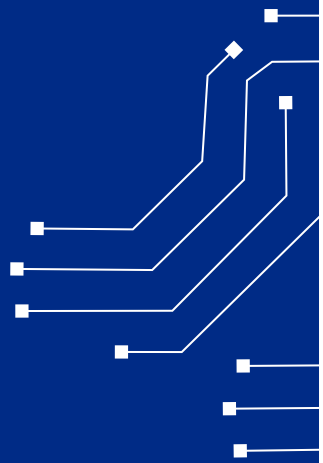
Results

The KATLAS team has installed CheriBSD and compiled a codebase for AArch64C (Morello). They have conducted bound checks to test fat pointer properties, and created a program for testing compartmentalisation (c18n). They are now studying a potentially new c18n model.

L3Harris

L3Harris is an agile global aerospace and defence technology innovator.

Location	Tewkesbury
Email	hello@L3Harris.com
Website	l3harris.com
LinkedIn	/l3harris-technologies



Scope of project

The company's DSbD project scope was to become familiar with the principles and technical details of CHERI memory protection and compartmentalisation, and evaluate the benefit to cyber security and the electronic warfare products that L3Harris develops.

Results

The porting of the compartmentalisation Morello examples from Android to CheriBSD was a success. Porting the compartmentalisation demo from the ARM-specific executive/restricted branching primitives to the standard CHERI sentry branching primitives was also successful.

Leo CybSec helps businesses to mitigate modern cyber threats, extending their security capabilities and implementing the latest best practices and cyber security solutions.

Location	London
Email	info@leocybsec.com
Website	leocybsec.com
LinkedIn	/leo-cybsec
Twitter	@LCybsec

Leo CybSec

Scope of project

The Leo CybSec project team wanted to understand if the attack surface has been reduced against a number of known critical vulnerabilities.

Results

They have identified a few compatibility issues with the exiv2 tool, as well as finding that some good security defenses were enabled. They are also now analysing how CHERI can enhance security for bento4.

MBDA UK

MDBA is a European defence company, designing and manufacturing complex weapons for all branches of the armed forces.

Location	Stevenage
Website	mbda-systems.com
LinkedIn	/mbda
Twitter	@byMBDA

Scope of project

MBDA's project is studying how the CHERI architecture could impact software design philosophies, and how it could support their need to meet required safety standards (for example, by enabling compartmentalisation of the different processes running on a device).

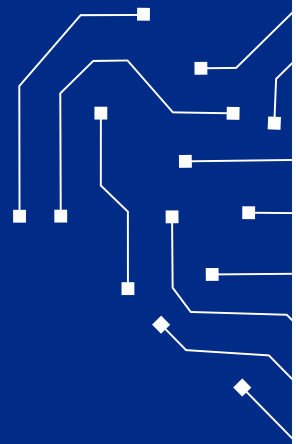
Results

Early work has focussed on getting the Morello board set up, ready to begin investigations. From work so far, it would appear that the CHERI architecture will allow finer-grained compartmentalisation than other similar software/OS based solutions, and could potentially provide better protection of low-level software.

Metrarc

Metrarc's ICMetrics generates unique identifiers for electronic devices, enabling secure encrypted communication between devices, regulating access, and reducing fraudulent activity.

Location	Colchester
Email	contact@metrarc.com
Website	metrarc.com
LinkedIn	/metrarcltd
Twitter	@Metrarc_Ltd



Scope of project

This DSbD project is focused on the practical implementation of Metrarc's Trusted Ring security product on the capability hardware prototype. This would enable Metrarc to showcase a hardware-based, higher TRL prototype demonstrator and evaluate the practicalities of adopting the Morello technology, in particular for use by military and communication partners and customers.

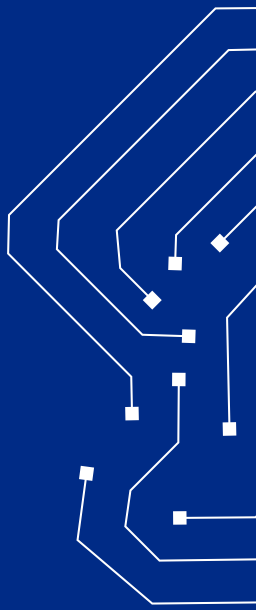
Results

The project used the existing communication infrastructure and services side of the Trusted Ring technology demonstrator. The team developed a suitable implementation of their ICMetrics technology for the Morello hardware board, enabling evaluation of the practical aspects of implementation.

Oxon Tech

Oxon Tech supports tech startups and provides bespoke R&D work for SMEs and government, enabling machine learning workflows from cloud data collection and model creation to edge processing on embedded devices.

Location	Kidlington
Email	info@oxon.tech
Website	oxon.tech
LinkedIn	/oxon.tech
Twitter	@OXONdotTECH



Scope of project

Oxon Tech's project investigates the use of DSbD within a tracking and situational awareness platform designed for fire and rescue, and defence/security use in the UK. This involved running their capability-enabled codebase on the Morello board, porting their system prototype code to run on CheriBSD, investigating hardware capabilities and support, and evaluating the system for stability and security.

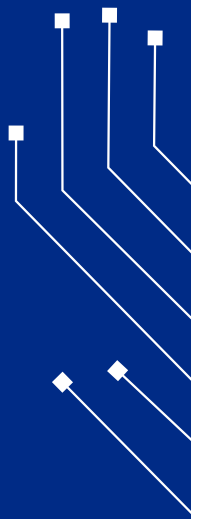
Results

CheriBSD has been installed, a hybrid mode FDTI library built and run, and a USB to I2C adapter set up. The team has also ported OpenVINO and compiled ROS2 to allow their original code to work on the Morello board, and made great progress in evaluating the use and impacts of the DSbD technologies. They have highlighted a few challenges, mainly around closed source hardware drivers and software not designed for BSD, but are working through them steadily.

Pytilia

Pytilia is a software consultancy with a focus on IT infrastructure, financial services and healthcare.

Location	Belfast
Email	neil.sinclair@pytilia.io
Website	pytilia.io
LinkedIn	/pytilia
Twitter	@pytilia_io



Scope of project

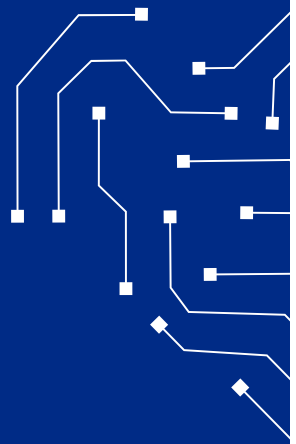
Pytilia is applying DSbD technologies to demonstrate a network application that delivers secure, high-performance packet processing. The project builds on Pytilia's initial success in the DSbD Software Ecosystem competition, with the goal of proving that CHERI capabilities can be used to deliver a 'best of both' solution for both performance and security. This would mean not having to prioritise one over the other, as is the case today.

Results

Results are positive and indicate that DSbD technologies deliver the targeted 'best of both' solution for performance and security. When comparing like-for-like applications implemented using traditional and DSbD approaches, the Pytilia team has seen that the DSbD approach delivers improved performance (for both latency and CPU utilisation) and the security benefits associated with CHERI capabilities.

The Systems Security Group at Swansea University is a multi-disciplinary research team addressing issues of systems security.

Location	Swansea
Website	swansea.ac.uk
LinkedIn	/swansea-university



SSG, Swansea University

Swansea University Prifysgol Abertawe

Scope of project

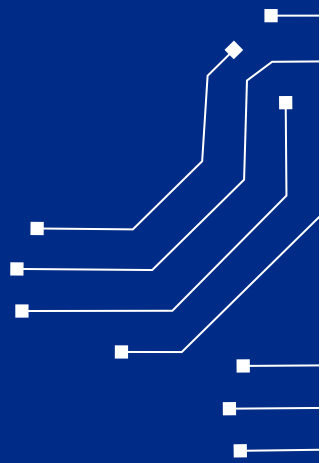
Through this project, the team is investigating the feasibility of employing the CHERI architecture to protect telematics functionality against buffer overflow attacks. This will involve the telematics control unit (TCU) implementation in Automotive Grade Linux (an embedded operating system for automotive) being ported to the Morello software stack.

Results

The expected result is to have telematics functionality running on the Morello board, so that in-vehicle engine data can be remotely monitored for diagnostic purposes.

Tot Ei works with major brands to evolve wireless communications ambitions into reality.

Location	Cambridge
LinkedIn	/alexdaniellungu



Tot Ei

Scope of project

Tot Ei's project is focussed on improving the security of Wi-Fi communications using avant garde security mechanisms. The main area of investigation is centered around the resilience of a wireless supplicant against over-the-air attacks.

Results

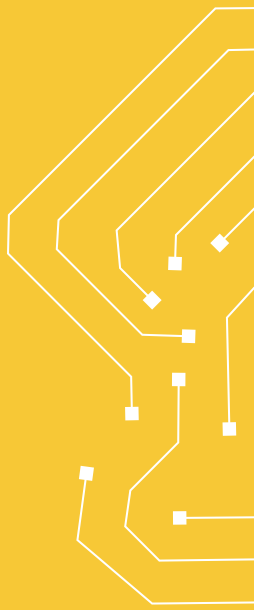
CheriBSD has been installed in pure-capability mode, and wpa_supplicant has been successfully ported, debugged and all libraries recompiled. Secure Wi-Fi connections can now be made on the Morello board.

Tot Ei is currently testing wpa_supplicant against known vulnerabilities to see how CheriBSD/Morello defends against them.

Greeve

Greeve provides bespoke electronic and software engineering, alongside design, research, and development services.

Location	Powys
Email	info@greeve.co.uk
Website	greeve.co.uk
LinkedIn	/greeve-ltd-
Twitter	@GreeveLtd



Scope of project

The DSbD project scope is to address memory leaks and vulnerabilities due to programmer errors, and to build a better awareness of security and stability using the CHERI/Morello architecture by porting the in-development ARWAIN codebase (a new localisation system). Greeve is focusing on identifying previously unknown issues with dependencies, to allow repair or elimination. They also intend to contribute fixes to the open-source community.

Results

Greeve identified a handful of code errors using the LLVM compiler in pure-cap mode. Within third-party libraries, the team discovered a number of issues with pointer alignment and misuse of integer types as pointers, which they are working to resolve. They are also preparing pull requests against the identified repositories, to start delivering value to the open-source community.

JET Connectivity

JET Connectivity provides resilient 5G connectivity at sea, driven by a desire to improve the environmental and safety impacts of marine, commercial, and leisure interactions.

Location	Farnborough
Email	hello@jet-eng.com
Website	jet-eng.co.uk
LinkedIn	/jet-connectivity
Twitter	@jet_systems

Scope of project

JET deploys floating 5G-enabled base stations that provide pop-up 5G communications for a range of offshore applications and sectors. This project uses the Arm Morello board with the 5G base station software to provide greater security and enhance JET's service offering, enabling a more secure network to be deployed for customers with highly sensitive data.

Results

The team has successfully ported over the 5G base station software, plus other software required, and they are now working on fixing bugs and making use of Morello/CHERI security features.

Mission Critical Applications

Mission Critical Applications (MCA) is an SME specialising in software for safety-critical systems.

Location	Bath
Email	enquiries@mca-ltd.com
Website	mca-ltd.com
LinkedIn	/mission-critical-applications-limited

Scope of project

The project scope is to port the seL4 microkernel to run natively on Morello with hybrid and purecap user space processes, and then measure the impact of capabilities in the seL4 environment. The goal is to create a proof-of-concept environment where the proven seL4 kernel is augmented by user space processes that are made safer and more secure through CHERI capabilities. The MCA team sees this as an ideal foundation for the use case of highly safe and secure systems.

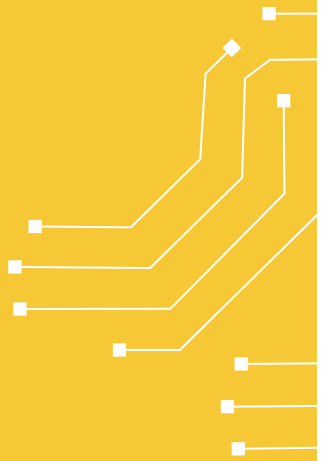
Results

The Arm Research IceCap project made the first steps to getting seL4 running on Morello last year. MCA is building on their achievements, porting seL4 from Qemu to the Morello hardware, and extending their work to support purecap userspace processes.

Prizsm

Prizsm enables anyone to easily protect and secure their information in the public cloud. Prizsm's unique multi-cloud distribution approach enables businesses to retain data more safely at all levels of security classification.

Location	Malvern
Email	info@prizsm.co.uk
Website	prizsm.co.uk
LinkedIn	/prizsm-technologies
Twitter	@prizsm_uk



Scope of project

Prizsm's project scope is to improve their existing application's hardware-software security architecture by porting as much of the existing C++ codebase as possible to run on the Arm Morello platform. Then to refactor elements that do not easily port over to the new architecture, or depend on external packages not available from the CHERI hardware software stack. The aim is to make data on the cloud as secure as possible by uncovering any vulnerabilities.

Results

The Prizsm software environment dependencies and toolchain have been deployed. The team has built dependant packages from source (cpprestsdk, aws-sdk-cpp, wt), and an initial test build of Prizsm's code modules (cloud, encryption, file splitting, filesystem, and UI) to create a triage list. The porting exercise has helped them reduce technical debt and is illuminating opportunities to improve the way code is implemented.

About

UK Research & Innovation

UKRI convenes, catalyses, and invests in close collaboration with others to build a thriving, inclusive research and innovation system.

Launched in April 2018, UKRI is a non-departmental public body sponsored by the Department for Science, Innovation and Technology (DSIT).

Our organisation brings together the seven disciplinary research councils, Research England, which is responsible for supporting research and knowledge exchange at higher education institutions in England, and the UK's innovation agency, Innovate UK.

Discover more at: **ukri.org**

UK Research and Innovation

Digital Catapult

Digital Catapult is the UK authority on advanced digital technology. Through collaboration and innovation, we accelerate industry adoption to drive growth and opportunity across the economy.

We bring together an expert and enterprising community of researchers, startups, scaleups and industry leaders to discover new ways to solve big challenges to unlock the UK's future potential. Through our specialist programmes and experimental facilities, we make sure that innovation thrives and the right solutions make it to the real world.

Our goal is to accelerate new possibilities in everything we do and for every business we partner with on the journey: breaking down barriers, de-risking innovation, opening up markets and responsibly shaping the products, services and experiences of the future.

Discover more at: **digicatapult.org.uk**

CATAPULT Digital

Thanks to all DSbD TAP delivery partners and cohort members

Partners

CATAPULT Digital

UK Research and Innovation

arm

University of Cambridge
Department of Computer Science and Technology

Cohort members

MBDA

IOETEC
ENSURING IOT DATA IS TRUSTED AND SECURED

cambridge consultants
Part of Capgemini Invent

telkoa
better mobile. better IoT.

JET CONNECTIVITY

VA

CHEVIN TECHNOLOGY

Swansea University
Prifysgol Abertawe

GREEVE SYSTEMS

Sensorit

MISSION CRITICAL APPLICATIONS

prizm

REALVNC

Metrarc

pytilia

RISKOA
SECURING A SAFE WATER FUTURE

Cedyr

OXON TECH
MANAGED IT SERVICES & SUPPORT

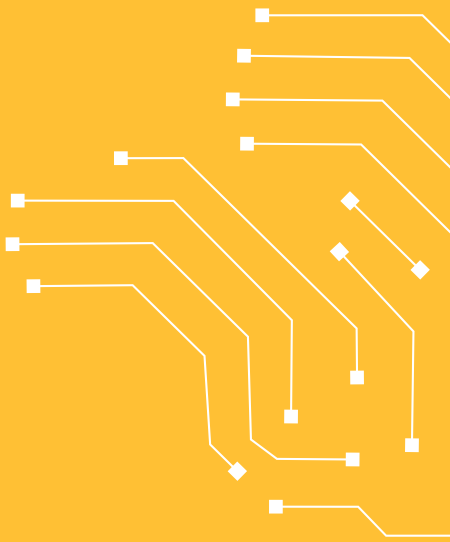
dynamicdevices LTD

L3HARRIS

3bian

KATLAS
Accelerating innovation

Digital Catapult is part of the Catapult Network that supports businesses in transforming great ideas into valuable products and services. We are a network of world-leading technology and innovation centres established by Innovate UK.



Digital Catapult
101 Euston Road London
NW1 2RA
digicatapult.org.uk

CATAPULT Digital

UKRI UK Research and Innovation