Digital Security by Design

Technology Access Programme

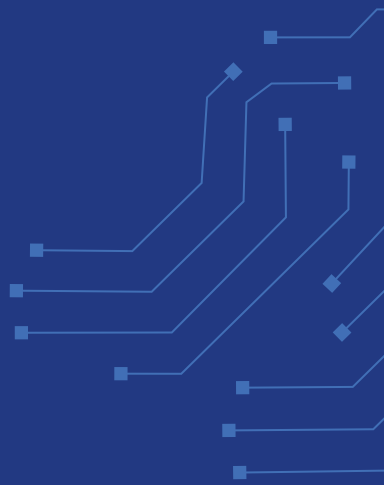
Showcase

22 November 2023
Hosted by Digital Catapult

Delivered by Innovate UK, EPSRC and ESRC

CATAPULT Digital

Website	dsbd.tech
LinkedIn	/digital-security-by-design
X	@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 Showcase is an event that celebrates six months 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.

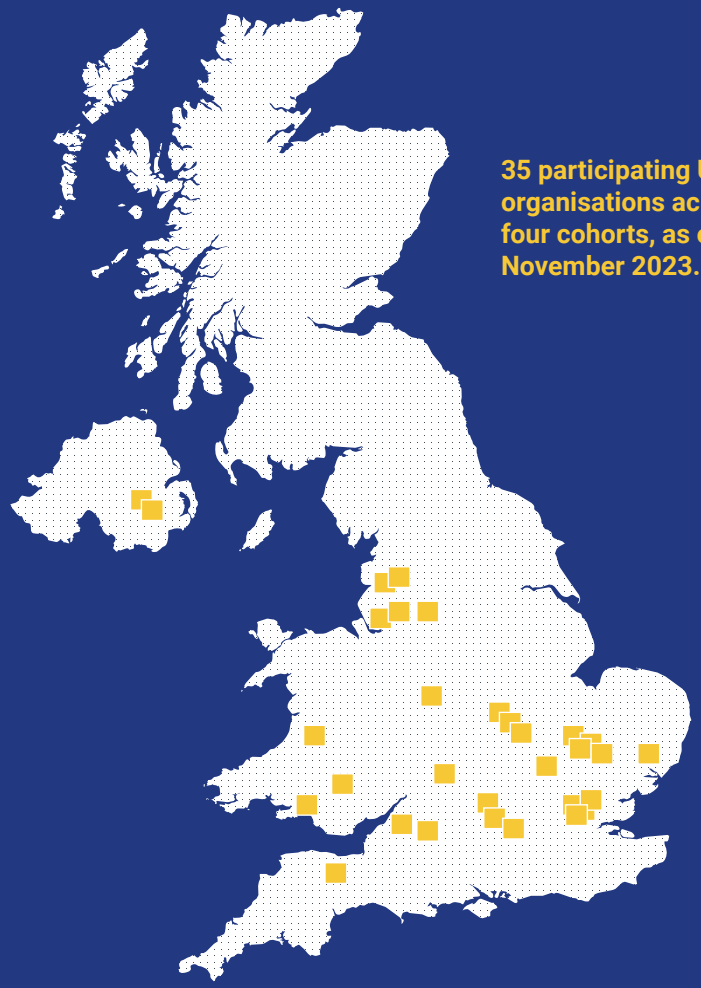
DSbD has been an essential part of this realisation, creating the first industrial-quality demonstrator of the CHERI concept, Arm's Morello prototype processor, SoC, and board. This has resoundingly validated a key hypothesis regarding the viability of the hardware approach.

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.



35 participating UK organisations across four cohorts, as of November 2023.

Programme scale so far

+15 million lines of code ported to Morello by Cohorts 1, 2, 3 and 4

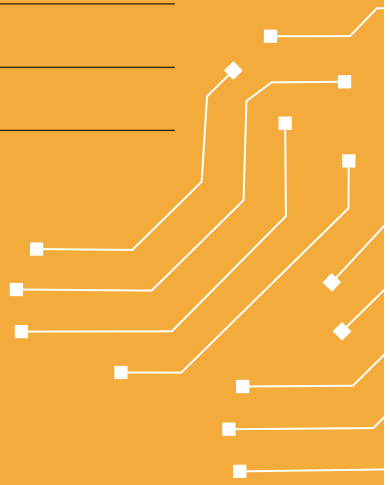
32 networking and learning events

Multi-sector and cross-discipline involvement

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

Configured Things provides the platform for building systems that safely spans trust domains and cross-domain systems automation

Location	Bristol
Email	getconfigured@configuredthings.com
Website	configuredthings.com
LinkedIn	/configured-things
X	@confthings



Configured Things

Configured THINGS

Scope of project

To evaluate the applicability of CHERI's memory protection model to the problem of building a cross-domain solution.
The platform makes use of diodes to break protocols and enforce strong verification of communications. Current solutions are too expensive and inflexible, using specialised hardware, for all possible use-cases. Their goals were to see if it is possible to make systems with appropriate security properties and at lower price points.

Results

Experiments to build a diode were carried out using CheriBSD solution on the Morello board, plus the cocalls variant in a QEMU VM and later using the Morello release. The cocalls model was the most appropriate, but the size of CheriBSD rules it out for such secure systems. CherIoT is a better choice, and further experiments have begun. Configured Things hope to test on a lowRISC board when it becomes available.

Systems Security Consulting delivers R&D and consulting in trusted computing, systems security, from embedded devices to clouds.

Location	Cambridge
Email	info@sys-sec.co.uk
Website	sys-sec.co.uk

Systems Security Consulting

Scope of project

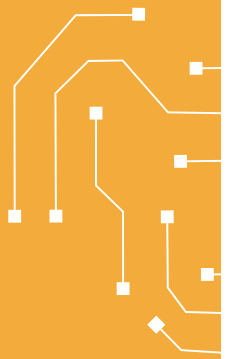
To extend Intravisor – the type-3 hypervisor that utilises hardware memory capabilities as the foundation for virtualisation – with cloud VM orchestration functionality. Their aim is to facilitate remote manipulation of Intravisor through software and simultaneously integrate this capability using cap-based compartments.

Results

Systems Security Consulting successfully ported cloud orchestration software libvirt to the pure-cap ABI, along with its dependencies. They integrated it with Intravisor as a stand-alone capability-based virtual machine and extended the hostcall interface to support cloud management functionality.

Ultra Cyber protects the most critical infrastructures with wired, wireless, and embedded encryption solutions forged by decades of cryptographic engineering accomplishments.

Location	Middlesex
Email	information@ultra-electronics.com
Website	ultra-ic.com/
LinkedIn	/ultra-electronics-group



Ultra Cyber

ULTRA | Intelligence & Communications

Scope of project

The original project aim was to port their existing C/C++ codebase and fuzz the application using American Fuzzy Lop (AFL), in the hopes of uncovering further CHERI exceptions and memory safety vulnerabilities. However, as no fuzzing tools were available for Morello, their plan had to be adapted to include porting AFL.

Results

Some of ULTRA's proprietary software has been ported to CheriBSD, and including the Barracuda web server. ULTRA has managed to port AFL to CheriBSD, to allow fuzzing on Morello. The code for this has been made publically available.

rtegrity delivers data agility and resilience through software development, research, consultancy and training.

Location	London
Email	info@rtegrity.com
Website	rtegrity.com
LinkedIn	/rtegrity
X	@rtegrity

rtegrity

Scope of project

rtegrity has been investigating how library compartmentalisation can be applied to the widely used Storage Performance Development Kit (SPDK) as part of a secured storage stack.

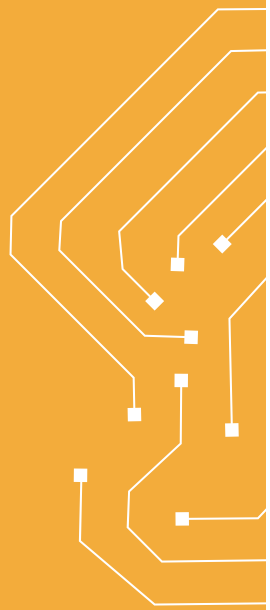
Results

Initial results indicate that library compartmentalisation has the potential to improve the security of the stack at an acceptable level of overhead.

ScienceScope

ScienceScope provides a collection of IoT tools, devices, and resources to users around the world across multiple sectors including Education, Industry and Academic Research.

Location	Bath
Email	enquiries@sciencescope.uk
Website	sciencescope.uk
LinkedIn	/sciencescope



Scope of project

ScienceScope planned to create a Building Management System (BMS) that is securely linked to the ScienceScope IoT platform, built on the Azure network. The CheriBSD software stack running on Morello forms the gateway to this BMS. The Morello board controls all aspects of the BMS, supporting data import from external systems, data export to the ScienceScope IoT platform and additional systems requiring integration.

Results

The primary goal of creating a retro-fit BMS system was achieved. The system was installed into a building without a BMS and started collecting data that could be transferred to the Azure based ScienceScope IoT Exploratory system. Future development will include interfacing more hardware, along with expanding the functionality of the code and implementing compartmentalisation.

TELXAI delivers UK-built 4G and 5G enabled CCTV cameras with integrated video analytics operating at the edge.

Location	Bristol
Website	telxai.com
LinkedIn	/telxai
X	@telxaitech

TELXAI

Scope of project

TELXAI's goal was to run a real-time video feed demonstrating a secure CCTV feed with integrated video analytics utilising the CHERI OS on top of the Morello board. Utilising executables that are at risk of out-of-bound writes, they generated and tested executables that could lead to the device being taken offline. These out-of-bound reads may lead to sensitive data regarding the rest of the security infrastructure being obtained.

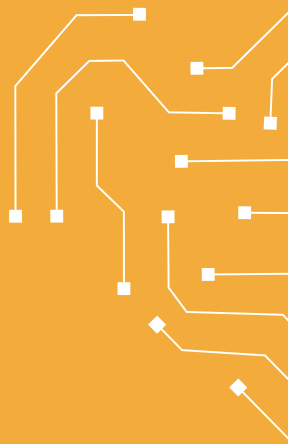
Results

TELXAI ported over 1,4 million lines of code and edited 148 lines of code from OpenCV to CheriBSD/Morello. TELXAI then tested this system against possible out-of-bounds read/write attacks. This was followed by testing with fuzzing and finally, TELXAI simulated the IP camera on Morello.

Goldilock Secure

Goldilock Secure provides physical network security for the critical national infrastructure and defence sector.

Location	Wolverhampton
Email	richardbate@goldilock.com
Website	goldilock.com
LinkedIn	/goldilocksecure
X	@goldilocksecure



Scope of project

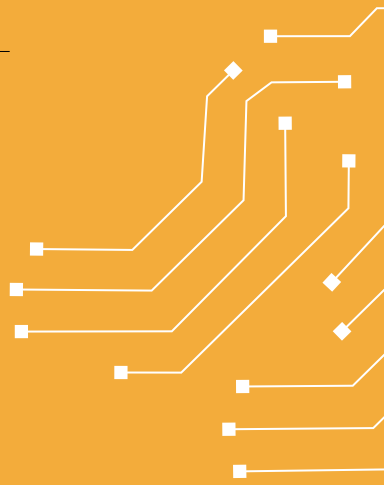
Goldilock's aim was to migrate their existing underlying C and C++ software architecture over to CHERI and assess the hardware capabilities as a candidate for their long-term hardware development roadmap. As a stretch-goal, they also explored the possibility of migrating over their front-end and API functionality written in NodeJS.

Results

Some minor refactoring was required to accommodate for the current maturity of libraries available. They experienced some limitations with NodeJS - as expected - and therefore decided to pivot to Python/QT for the demo user interface.

Secure Compute Institute (SCI) Semiconductor is a startup looking at how RISC-V and CHERI extensions can impact secure computing at a truly global level.

Location	Cambridgeshire
Email	info@scisemi.com
Website	scisemi.com



SCI Semiconductor

SCI Semi

Scope of project

SCI Semiconductor wanted to investigate how CHERI extensions can support IoT devices by demonstrating CHERIoT on an FPGA device.

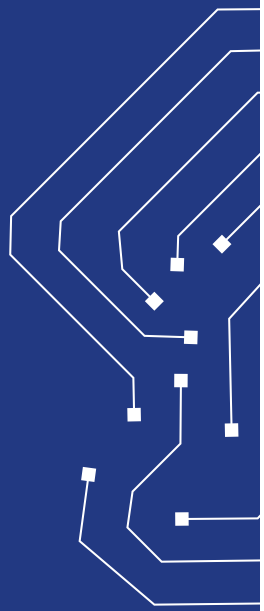
Results

They have ported CHERIoT RTOS onto an FPGA and were able to run some code on this new device. They are documenting the porting process in a user guide for other new users.

Sensor IT

Sensor IT is an innovative IoT technology provider and manufacturer that develops solutions for critical IoT verticals

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



Scope of project

Sensor IT ported a bug-ridden, complete software suite, an email server (eXtremail), to the Morello Board/CheriBSD platform, in order to prove how this exercise enhanced the security around all basics operations of the server. Following this, the suite was compiled using CheriBSD's library-based memory compartmentalisation functions, in order to verify any potential performance issues, if any, associated with the new memory management model

Results

Sensor IT was able to verify that only by porting the server code to the Morello Board/ CheriBSD platform completely eliminated all critical security bugs that affected the software, more specifically, remote code execution based on memory overflow. With respect to memory compartmentalisation, the drop in performance was negligible – less than 5%.

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**

Delivered by Innovate UK, EPSRC and ESRC

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**

Thanks to all DSbD TAP delivery partners and cohort members

Partners

UKRI Delivered by Innovate UK, EPSRC and ESRC

CATAPULT Digital

UNIVERSITY OF CAMBRIDGE Department of Computer Science and Technology

arm

Cohort members

Configured THINGS

SCI Semi

science scope

ULTRA Intelligence & Communications

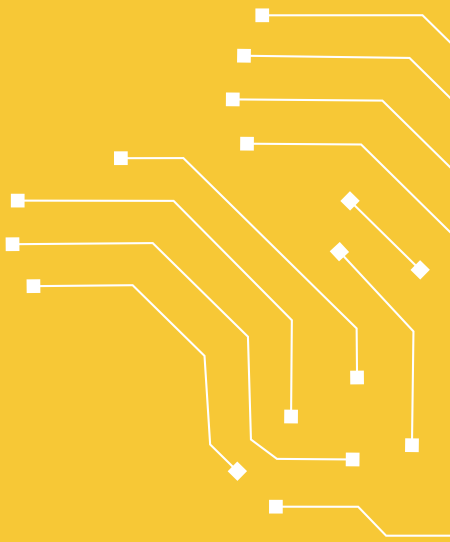
rtegrity

TELxAI

goldilock

Sensorit

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

Delivered by Innovate UK, EPSRC and ESRC