UK Research and Innovation

Digital Security by Design

Mid-Term Report 2023

Digital Security by Design (DSbD) is an initiative supported by the UK government to transform digital technology and create a more resilient, and secure foundation for a safer future.

Foreword

Professor John Goodacre
DSbD Challenge Director

The costs of cybercrime are reaching the trillions of dollars globally each year. As the amount of software grows, attack surfaces grow. Vulnerabilities occur from the way we design, build and use technology, with technology doing little to protect us by design. It is becoming clearer that cyber security practices as they currently stand are becoming unsustainable to deal with attacks and we must change the fundamental technology to block exploitations and limit the opportunities for data loss and ransomware.

In 2019, the exciting Digital Security by Design programme was established to unlock research and enable industry with the objective to fix the foundations and realise technical developments, the size of which computing has not seen for 50 years or more. The new approach will protect software through the silicon design of the hardware so that systems are more secure by design, rather than built on a foundation of sand.

An intervention change of this scale was required because of a substantial market failure that prevented any single industry from being able to drive the required changes. That is, a hardware manufacturer would not build a chip if there would be no software to run on it, and software companies would not write any new software if there were no chips on which to run it. Over the last three years, the DSbD programme has convened the relevant communities and industries to bring software and tools together with a prototype chip and overcome the market failure. The programme has enabled the underlying hardware security research from University of Cambridge, known as CHERI, to be prototyped in a mainstream Arm processor through their Morello Board and made available across the community. This has allowed industry users and researchers to evaluate the boards ability to prevent the exploitation of two thirds of ongoing vulnerabilities, while finding new ways to secure and increase the resilience and safety of new software designs.

As we overcome the fundamental market failure, it is still imperative that UK Government, industry, academia and international partners continue to work together to develop this ecosystem further by driving forwards adoption of this ground-breaking approach to protecting the cyber world, while also applying the secure by design approach to areas of potential future attack.

Foreword

Richard Grisenthwaite
Executive Vice President and Chief Architect, Arm

Arm believes that security is the greatest challenge that computing needs to address to meet its full potential. Arm technology is used in products that are transforming every industry by enabling access to data and communications, and by extracting information and meaning from that data. This transformation continues in our society wherever the application of computing resources can make people's lives easier and more connected. Unfortunately this increasing reliance on computing has created unprecedented opportunities for criminals, as can be seen in the ever-growing cost of cybercrime. In addition, the growing reliance of national infrastructure on technology means that computer security is a crucial element of National Security. Given this context, it is reasonable to assert that the boundaries of the computing revolution will be determined by the security of our computing systems.

There is ample evidence that memory safety issues such as buffer overflows and use-after-free have been a persistent source of vulnerabilities for many years, and this continues in many ecosystems. Such memory safety issues form the basis of around 70% of reported security vulnerabilities at a remarkably consistent rate for the past few years. While languages such as Rust offer the prospect of more inherent memory safety, the reality is that there is a huge body of C and C++ code being used, written, and adapted every day, and there are many undetected vulnerabilities waiting to be exploited. While a variety of techniques have been used to identify these memory safety issues before they are exploited, it would undoubtedly be better if computer designs were inherently more robust against these issues.

The promise of CHERI capabilities is that they introduce a new architectural concept that fundamentally provide resilience against buffer overflows, and can be used to construct mechanisms for protecting against use-after-free issues. Even more significantly, the technology can be used to construct much more fine-grained compartmentalization than can be achieved by other approaches and this will allow software to be much more resilient against attacks as and when they do manage to be exploited. Theoretical studies have shown that this technology has the ability to prevent around two-thirds of the vulnerabilities that have led in the past to security patches to software in the field. Those sorts of potential improvements are far greater than have been seen from any other technology and shows the potential value of this technology.

The Digital Security by Design Program has enabled the creation of Morello, a very high performance demonstrator of this technology, to be designed and manufactured, and for it to be made available to a wide range of researchers to allow a much more complete evaluation of this technology for a wide range of real software workloads and environments. This is an unprecedented opportunity to establish the whether the real-world benefit of this technology is sufficient to enable its deployment. It allows researchers in both academia and industry to try out a range of different approaches in their software to allow the design of a commercially viable form of the technology, and to enable the establishment of the real value of this technology. The wide availability of the Morello systems and the funding of the research for using the technology will enable Arm, and other processor companies, to really understand the value of this technology, and so work towards having computer systems that are inherently more secure by design.

The Digital World We Live In

We live in a world that is increasingly underpinned and influenced by the technology we use. From social media and online shopping, to our water and gas supplies, almost everything we touch or use, relies in some way on the digital world. This is only set to grow in the coming years.

This presents great opportunity for creating new ways to live, work and play. With the opportunity, however, comes a greater risk of exposure from an ever-growing attack surface. This exposure is amplified by the use of software which has increased exponentially during the last few decades, leading to over 2.8 trillion lines of code today. [5] With just a single mistake in code, a system could be exploited by an attacker with disastrous consequences. As the number of lines of code continue to grow and the exploitation of vulnerabilities becomes more prevalent, we could be heading towards a cyber disaster. That is, unless something is done to help block exploitation by design.

Average UK household has **nine** consumer connectable products. [6]

Every second, **127** devices hook up to the internet for the first time. [1]

2.8 trillion lines of code. [5]

In 2017, 27 billion devices were connected using IoT. This number is expected to increase to **125 billion** by just **2030**. [2]

The semiconductor industry shipped a record **1.15 trillion** semiconductor chips in 2021. [3]

(Semiconductor Industry Association

By 2030, about **95 percent** of new vehicles sold globally will be connected. [4]

Cyber Security Today

As it stands, cyber security is a battle between a continuous escalation of attacks against a defence of keeping up with your software patching and attack monitoring.

For decades, computers have been vulnerable due to design errors and bugs in software, resulting in data breaches and organisations being held to ransom. The world of cyber security has evolved around knowing if you are being attacked, and managing those risks, as opposed to blocking or removing any fundamental issues in a computer's design.

In addition to the ever-expanding attack surface and highly reactive approach, a growing skills gap [6] is raising its head leading to an ever more fragile security ecosystem. 54% of organisations are highlighting that cyber-attacks are now too advanced for their IT teams to handle on their own [7] causing burnout and compounding the cyber risk.

To continue as we are is unsustainable, if we continue to only treat the symptoms of the attacks rather than finding the vaccine, then the failures of cyber security will only continue to grow with some anticipating the global cost of cybercrime to exceed $10 trillion by 2025. [8]

"Today, every computer from a massive cluster training a machine-learning model in Azure down to a microcontroller in a smart lightbulb is connected to the Internet. Every Internet-connected device is exposed to attackers, ranging from bored teenagers to experienced professionals backed by organised criminal organisations or rogue states. In this climate, being able to deterministically mitigate the most significant classes of vulnerabilities is not just valuable, it is essential for critical infrastructure."

- Microsoft

The Impacts of Cyber Security Failure

The impacts of cyber security failure vary from vaguely annoying right the way through to life threatening. The range of personal, financial and business impacts they may have include:

- Theft of personal, financial and medical information
- Damage to reputation
- Emotional and health impacts
- Loss of earning due to downtime
- Loss of competitive advantage through Stolen IP
- Loss of customers through loss of trust
- Reduced sales, profits and productivity
- Negative stock market reactions
- Broken relationships with partners and investors
- Legal costs
- Fines

The Failures

The World Economic Forum lists failure of cyber security as a **top risk** [1]

39% of UK businesses identified a cyber attack [10]

Cyber criminals in Florida **accessed critical national infrastructure**, changing the chemical levels of the water supply sparking health concerns [12]

31 % of businesses estimate they were attacked at least **once a week** [10]

1 in 5 say they experienaced a negative outcome as a result of an attack [10]

Cyberattacks on IoT devices surpassed **300%** in 2019 [1]

48% of businesses are unable to detect IoT security breaches [1]

Hackers remotely accessed a car braking system while on the highway raising significant safety questions about connected vehicles [13]

1.5 billion attacks against IoT products in the first six months of 2021 [11]

What is UK Government doing about it?

UK government has already legislated the Product Security and Telecommunications Infrastructure Bill (PSTI), the first and most advanced of its kind in Europe. This is leading the way to products being shipped more securely by default through:

- Banning default passwords.
- Requiring products to have a vulnerability disclosure policy
- Requiring transparency about the length of time for which the product will receive security updates.

The release of the National Cyber Strategy 2022 (NCS) acknowledges that more needs to be done. Placing additional security obligations on software manufacturers through the PSTI bill is only part of the solution. Therefore, as part of the NCS, 5 pillars and priority actions have been created:

1. Strengthening the UK cyber ecosystem
2. Building a resilient and prosperous digital UK
3. Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies
4. Advancing UK global leadership and influence
5. Detecting, disrupting, and deterring adversaries

Taking the lead in the technologies is the key pillar where the Digital Security by Design Programme (DSbD) has been able to influence the UK Cyber Strategy and support the development of a safer future.

From the NCS the Government Cyber Security Strategy was subsequently released in 2022, highlighting the UK Government ambitions for its own functions. If the Government wants to achieve the aims set out in the strategy, namely that –

"Government's critical functions will be significantly hardened to cyber-attack by 2025 and we will ensure that all government organisations across the whole public sector are resilient to known vulnerabilities and attack methods by 2030" then fundamental innovative new technology must be developed.

That's why UK Government, through UK Research and Innovation, DSIT and NCSC, are working together on the £300m Digital Security by Design Programme made up of £80m public funding and more than £200m industry co-investment.

> **"Future digital infrastructure can potentially enable our connected society to operate more safely, efficiently and sustainably. In order to deploy new technology with confidence, vendors will need to satisfy users and regulators that their products and services are resilient against a range of attacks that threaten safe operation. The risk of exploitation at scale cannot be ignored.**
>
> **The DSbD programme aims to secure the foundations of future devices, reducing the impact of software vulnerabilities and hence the effort required to mitigate them. Responsible businesses with a long-term view should be taking a keen interest in how device resilience is being built in to their supply chain. Are your suppliers building on secure foundations?**
>
> Paul Waller – Principal Technical Director at National Cyber Security Centre

What is Digital Security by Design?

The way today's computers work can be traced back to the designs developed in the UK during the 1940's and 50's. Since the 1970's academia and industry have documented major issues in keeping data safe and secure, and maintaining resilience. Currently, bugs in software can lead to vulnerabilities in a digital product or service which can be exploited by individuals, organisations, or state sponsored groups, and, if we are to accept that to be human is to be imperfect, then mistakes will continue to be made in software and these will continue to be exploited at huge economic cost.

Unfortunately, a substantial market failure had prevented any single industry from fixing the documented problems. Essentially, new hardware would not be built unless there is software justifying its creation and software would not be created for hardware that does not exist.

The current timing, technical capabilities, industry backing, and UK government engagement has enabled an opportunity for DSbD to help overcome the market failure. Developing the foundational technology and software enablement in tandem to address vulnerabilities in ways not considered possible before while allowing developers to also increase the overall performance of their solution.

£80m
public funding from UKRI and UK Goverment

Matched by more than **£200 million** from industry

65 projects across academia and industry

Building **trust**

Increasing resilience, safety and security of products and services

Lowering the costs of security

Increasing **productivity** across development, maintenance, and management

Preventing the exploitation of around **70%** of ongoing vulnerabilities and enabling developers to further extend the resilience of software.

...Changing the world

Through its pioneering activities, the DSbD Programme is;

Demonstrating
a more secure hardware platform

Enabling
more secure platforms through the development of the software ecosystem

Accelerating
the move towards digital transformation of industry

DSbD is building on the hardware concepts of the CHERI research from University of Cambridge. The programme has funded, a collaboration between semiconductor and software design company Arm, University of Cambridge and University of Edinburgh to create the technology prototype known as the Morello Board.

With this new design, research suggests it is possible around 70% of ongoing memory safety vulnerabilities should be blocked from exploitation, with other features enabling developers to further extend the resilience of software.

The programme was split into multiple activities to ensure a holistic approach was taken to break the market failure and move towards a more secure world:

- Enabling prototype development
- Ecosystem and tools development - To enable market use, tooling and processes to utilise the new security capabilities
- Demonstration and industrial impact

No one organisation can make this change. The success of this movement depends on the sum being greater than all the parts. Only together can we make this change the success it needs to be.

Enabling the fundamental technology

CHERI: University of Cambridge

For over 10 years, the University of Cambridge has been refining its research into a new way of designing computer hardware known as CHERI. At a high level, CHERI has two features relevant to multiple architectures including Arm and RISC V:

- It revises the architectural interface between hardware and software to reinforce the structure of software, making it is less fragile and more resilient to attacks without requiring large scale changes to existing software
- It allows fine grained software compartmentalisation, meaning that if there was a successful attack, the attacker would gain as little information as possible.

In 2015, the University of Cambridge presented this research to Arm who took an interest in the opportunity this could provide the entire world of computing. Following reviews of the new designs, Arm along with the University of Cambridge and other industry and academic players, worked with UKRI's Industrial Strategy Challenge Fund to help break through the market failure once and for all.

Morello Board

Morello Program: Arm

As the provider of the processor architecture reaching more than two thirds of the world's people, Arm is uniquely positioned to bring the best and brightest of the industry together to prioritise security in next-generation technologies across all hardware platforms.

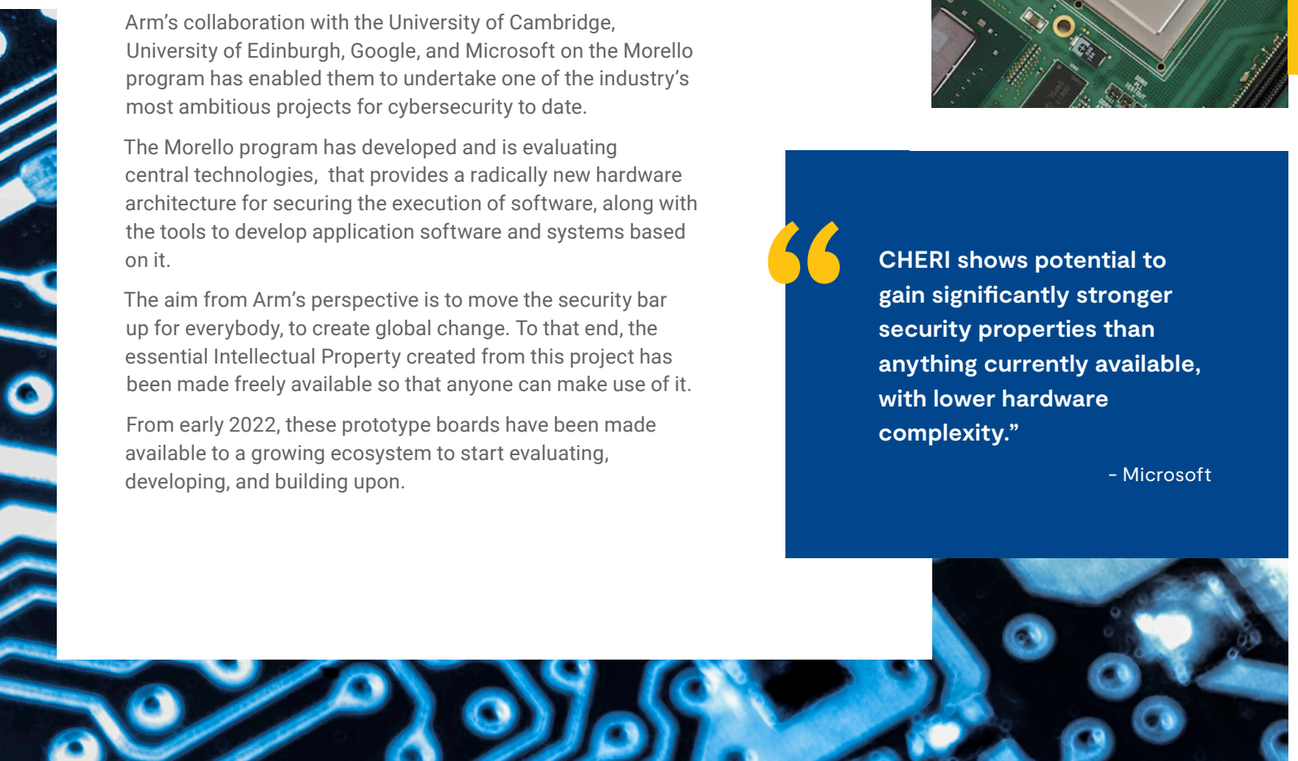
Arm's collaboration with the University of Cambridge, University of Edinburgh, Google, and Microsoft on the Morello program has enabled them to undertake one of the industry's most ambitious projects for cybersecurity to date.

The Morello program has developed and is evaluating central technologies, that provides a radically new hardware architecture for securing the execution of software, along with the tools to develop application software and systems based on it.

The aim from Arm's perspective is to move the security bar up for everybody, to create global change. To that end, the essential Intellectual Property created from this project has been made freely available so that anyone can make use of it.

From early 2022, these prototype boards have been made available to a growing ecosystem to start evaluating, developing, and building upon.

> **"CHERI shows potential to gain significantly stronger security properties than anything currently available, with lower hardware complexity."**
>
> - Microsoft



Ecosystem Development

With the Morello boards now available, the remainder of the programme has focused on providing proof, expanding and enriching the ecosystem to break the market failure, ensuring that the relevant tools are available for the future to enable adoption and creating relevant use cases.

This has translated to project workstreams focusing on fundamental research, early industrial investigation, software enablement and demonstrator use cases. The projects created for these workstreams are a result of competitive calls for proposals through UK Research and Innovation.

EPSRC Digital Security by Design Research Projects

Fundamental research projects started in 2020 following an EPSRC call seeking initial in the following areas:

1. Capability enabled hardware proof, formalisation and verification of software
2. Impact on system software and libraries
3. Future implications of Capability Hardware

The projects have been:

- Enabling for the first-time implementation of full stack security principles
- Securing multi-tenant environments in the cloud
- Securing essential foundational software frameworks
- Securing broader components of a computer
- Opening the benefit of secured execution to all developers
- Enforcing the intent and operation of computers
- Automating delivery of secure and correct applications
- Building confidence in code correctness

SME Early Investigation Projects

It was recognised that to encourage industry to start to look at the technology early, particularly SMEs, funding was required to start to engage audiences. A Fixed Virtual Platform was made available in 2020 for organisations to begin to review the technology. Through Innovate UK, the DSbD programme provided SMEs 6 months of funding to allow them to investigate the technology and its potential applications to their own products or services.

These projects concluded in 2021 and identified that, with "**minimal code change**", there may be "**productivity benefits**", "**potential commercial benefits**" of future adoption through market differentiation and potential for "**speed and power efficiency gains**" through new ways of working with the technology. For these SMEs and the DSbD Programme, this was a valuable learning exercise to understand the new technology. One significant outcome was the understanding that this could lead to a "**significantly more secure desktop**".

Software Ecosystem Development Projects

A larger scale ecosystem development competition was launched in 2021 encouraging bids from industry and academia to enrich and expand the DSbD software ecosystem. Start dates coincided with Morello board availability, meaning projects would be provided with boards to enable large scale, true to life testing and development to take place.

A synopsis of their anticipated impact is listed below:

- Securing desktop environments
- Hardened network router software increasing security and data protection
- Reduced attack surface for malicious attempts to subvert the expected control-flow
- Enable cloud providers to offer new trusted services
- Reduced memory footprint due to the fine-grained memory protection
- Enhancing the rust compiler to further benefit from compartmentalisation and protection of unsafe code.

Industrial Demonstrator Projects

The outcomes from the ecosystem development projects focus on enabling the benefits of the technology. To see this technology through to adoption however the programme defined that the benefits must be seen through sector specific lenses and we must be able to highlight the 'technology benefits' to those delivering products and services. To that end, the DSbD demonstrator competitions were announced, the first in 2020 and another in 2021.

The sectors focused on by the successful demonstrator projects are:

- E-commerce
- Automotive
- IT/OT Edge Cloud Infrastructures
- Critical National Infrastructure
- Telecoms

E-commerce

Soteria

Demonstrating the security capabilities of the Morello system in the e-commerce vertical industrial segment

THG Holdings PLC
The University of Manchester
University of Oxford

The Soteria demonstrator project is investigating, evaluating and demonstrating increased cyber security through the use and deployment of DSbD technologies in the e-commerce industry segment. This spans across The Hut Group's (THG) end-to-end system offerings from e-commerce software and data analytics to global logistics and hosting services.

The project is investigating how the OpenJDK-JVM can take advantage of the new CHERI-based hardware security features of Morello.

The Soteria project also focuses on social an economic benefits with respect to reducing the potential impact of security breaches and attacks, as well as the costs required and cultural blockers to secure digital businesses and services.

Expected benefits of the new technology include:

- Improved security for THG's e-commerce services
- Increased societal perception and trust in THG's technology
- Shorter time-to-market
- Reduced recovery time after a cyber security incident
- A secured by design e-commerce platform as a basis for protecting against future cyber-attacks

Automotive

AutoCHERI

Securing connected vehicles with Digital Security by Design technologies, a market demonstrator and study

Beam Connectivity Limited
University of Exeter
Coventry University
CSA Catapult
IDIADA Automotive Technology UK

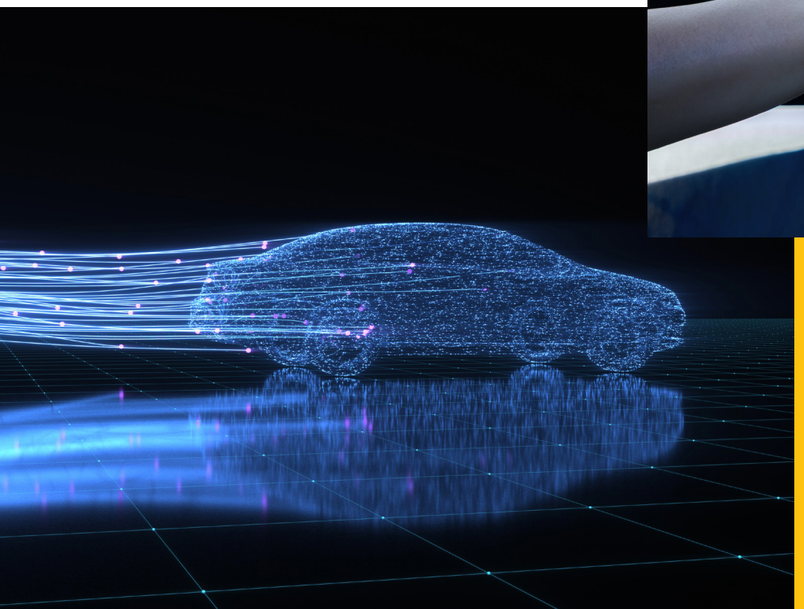
The AutoCHERI project is investigating the use of DSbD technologies for increased security and safety in the automotive sector with an increasingly software defined and network connected road vehicle and associated infrastructure. AutoCHERI will develop a Morello-based Telematics Control Unit (TCU) with enabling software and will showcase it across four connected vehicle use cases in real-world testing facilities:

- Over the air software updates;
- Vehicle to cloud diagnostic data communication;
- Infrastructure to vehicle traffic or accident ahead advisory communication with vehicle acknowledgment;
- Vehicle remote control and teleoperation.

The project will also examine the automotive regulatory environment with the step-change effect of DSbD technologies and will work directly with automotive OEMs to explore pathways to deployment and commercialisation.

Expected benefits as a result of AutoCHERI include:

- Reduced development time for a DSbD-based TCU
- Increased understanding of how DSbD technologies impact automotive testing, homologation, and legislative processes.



IT/OT Edge Cloud Infrastructures

MoatE

Morello at the Edge

Iceotope Technologies Limited
The University of Manchester

The MoatE project is investigating emerging cyber security and data protection challenges that are triggered by the increasing shift to edge computing. The underlying problem that the project aims to address is that edge facilities comprise several disparate networks, facility infrastructures and IT/OT hardware management systems that are traditionally siloed preventing a holistic monitoring and control view from a security standpoint.

This Operational Technology (OT)/ Information Technology (IT) divide entails a cultural / adoption mindset and a technology enablement challenge. At the heart of the MoatE demonstrator lies a new software-defined Secure-Edge-Facility-Orchestrator (SEFO) that will use CHERI-based memory protection capabilities as a steppingstone to showcase the potential of IT/OT infrastructures to co-exist securely and symbiotically while using converged resources. MoatE is the first business-led demonstrator to investigate how DSbD technologies can be deployed across the full edge-facility software/network stack.

Expected benefits resulting from the MoatE demonstrator:

- Enhancements in security (both virtual and physical), of a broadening attack surface
- Reductions in power consumption and CO2 emissions
- Improvements in resilience and fault run-through
- Improvements in maintenance and predictive maintenance in a broadening asset estate
- Better enablement of secure edge computing, through integration with existing building infrastructures

Critical National Infrastructure

DEFGRID

The Utility DSbD Demonstrator

Southern Gas Networks PLC
University of Strathclyde
Deltaflare Limited

The DEFGRID project addresses cyber security challenges of the critical national infrastructure (CNI) utility sector that is undergoing digital transformation in view of net-zero aspirations. The project, led by Southern Gas Networks PLC, leverages an existing industrial IoT edge platform, Phoenix, to strengthen its security using the DSbD technologies.

Two operational capabilities will drive the project use cases in terms of real-time sensor-to-cloud connectivity for remote operation and bi-directional data exchange; and connected process automation and control with remote update and management. Demonstration and validation will be performed at a utility-scale test environment (the Power Networks Demonstration Centre) with a further two physical demonstrators at operational SGN facilities.

In adding the secure by design operational capabilities the project expects benefits in terms of cost reduction for the consumer by reducing the burden on the gas supplier in terms of:

- Reducing in the need for manual intervention
- Improvement in process optimisation and delivery of energy efficiency
- Data driven, preventive and predictive maintenance
- Better capability to balance the network load through demand side response

Telecoms

High security communications infrastructure using peer-to-peer Mesh VPN

CyberHive
University of Oxford

Following on from their SME investigation Cyber Hive followed up with Mesh VPN demonstrator that focuses on cloud and network security and integrity that is relevant to many application domains requiring security-critical service, device connectivity and in-flight data protection beyond traditional enterprise use cases.

The project will redefine traditional approaches to VPN by enhancing a scalable solution employing low-latency mesh networking and post-quantum cryptography to benefit from CHERI enabled protection. Furthermore, the project is set to develop a framework and associated toolchain that will enable developers to use the Rust programming language when developing applications on the Morello hardware platform.

The project demonstrator aims to eliminate some of the vulnerabilities inherent in a software only VPN solution by limiting at a hardware level how specific segments of the Mesh VPN code are compartmentalised to ensure continued operation, even if successfully compromised by cyber-attacks.

Expected benefits of the new DSbD enabled Mesh VPN technology include:

- Improvement in productivity (higher network uptime, lower latency)
- Increase in deployment efficiency and mitigation against vulnerabilities and attacks on endpoint devices
- Applications that can benefit from this beyond state-of-the-art Mesh VPN technology include manufacturing, autonomous vehicles, utilities, military, and critical service infrastructure.

To see all project webpages, scan the QR code

Understanding Adoption through the Discribe Hub+

The adoption of technologies cannot rely on technical ability alone.

To aid the awareness and sociotechnical understanding of the barriers that stand in the way of next generation digital security success, the **Discribe Hub+** was funded in early 2020.

This community of social scientists, economists, computer scientists, and arts and humanities professionals bring diverse thinking together to help realise the possibility of a secure digital future for all.

To view the Discribe website scan the QR code here

Core Research

Overarching Goal

Work Plan

Adoption	Readiness	Regulation and Policy	Social, Cultural and Commercial Sector Differences
What are the barriers and enablers of adoption of new security technologies?	**Where does DSbD add value? How can that be best used?**	**To identify the ways in which a regulatory framework can best support DSbD and the challenges to achieving this**	**To understand: (i) differences in perspectives on the risks and opportunities of DSbD across commercial sectors; (ii) the relationship between perspectives and adoption**
Review of investment models (beyond Gordon-Loeb) Incentives and barriers across groups Quantify externalities Social norms and market failure	Scoping for HW insecurities in test-beds, working with DSbD projects to test interventions SW developers understanding and capabilities Users mental models of HW capabilities and security	Scoping / Reviewing regulatory models in (cyber)security Work with Gov / Industry on regulation, externalities, levers Case studies of policy & organisational culture	Large scale survey of industry & focus groups Ongoing collection of digital data for analysis of attitudes, adoption Cybercrime reduction and stakeholder perception

Commissioned Research

Assessing organisational DSbD awareness and readiness

Secure hardware adoption in the open data context

The impact of cyber security on the adoption of new digital technologies in UKs SMEs

The elicitation of cybersecurity narratives bricoleur story completion decision making and security

Using DSbD in practice: Is it a piece of CHERI-cake?

Regulation, Policy and Cybersecurity

Economic & Consumer Chain Analysis of Security

Regulatory Interactions & the Design of Optimal Cybersecurity Policies

Creating a Global Impact

Engagement

Early in the programme, the awareness and engagement had primarily focused on the UK tech community. In doing so, we have created a collaborative ecosystem across the UK with the best minds working on enabling various aspects of DSbD technology.

A unique nomenclature has been created in the programme to track and discuss the growth of the ecosystem around the technology.

Programme engagement activities across UK government, industry sectors and academia, has made it clear that now is the time to engage and overcome the challenges faced for so long in the digital world.

Going forward, DSbD Programme engagement will focus on amplifying communications with a sector specific narratives into the commercial, engineering and R&D teams across the telecoms, defence, and automotive as well as IoT/Operational Technology domains. The purpose of this engagement is to work with sectors who have the strongest strategic need and readiness to adopt the DSbD technology to move it forward. Value propositions, tailored use cases and stakeholder influence from across the ecosystem will be utilised to position the benefits of the DSbD technology, enabling decision making at executive levels.

The programme team will continue to work with Government and industry stakeholders to highlight the opportunities DSbD technology will bring, the need for the DSbD approach and provide the answers for accelerated adoption.

We will proceed with a focus on three levels of engagement:

Driving Demand

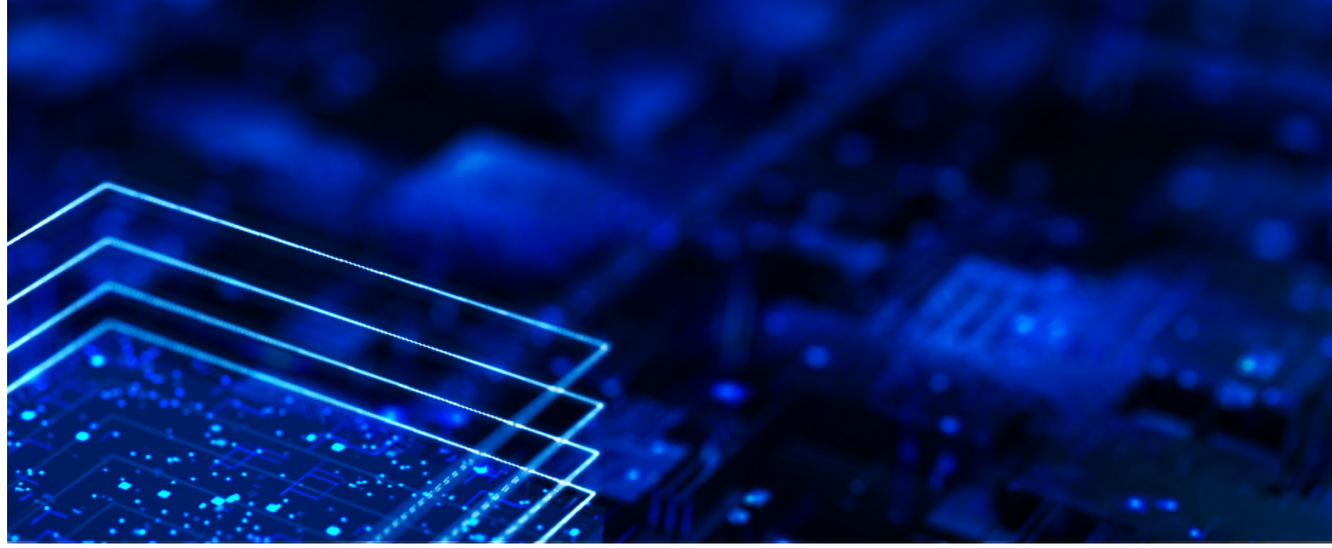
Driving demand for greater security, safety, resilience and integrity.

Technical accessibility

Feeding the ecosystem with the relevant documentation and pages.

Government Support

Considering future government levers.



UK Cyber Power

DSbD have been funding UK companies to ensure that this technology is recognised, supported, and developed in the UK, building on the progress towards making the UK a cyber power.

The Programme has also been supporting the distribution and use of Morello boards through its Technology Access Programme (TAP) run by Digital Catapult.

Technology Access Programme Participants

This programme has so far supplied an additional 27 organisations with boards for short term projects analysing and evaluating the board. These organisations have been keen to get involved early with a view of finding viable applications and, once commercially available, give them a first mover advantage in adopting the new technology, therefore differentiating their products from the market. Those engaging have also found more immediate benefits in building networks via an exciting group of organisations who are already involved, and have even found vulnerabilities in their production code just from compiling to the new technology.

TAP cohort members have generally seen benefits that the technology can bring to industry and to software development. Primarily the ability to "catch unanticipated errors and weak programming practices", as well as to block buffer overflows and "protect against code injections". An interesting mention has also been given to the potential for Morello to reduce the cadence of software patching requirements, thereby reducing time, costs, and resources required to develop and put out these patches.

International

To be deliver the full promise of this technology, it will ultimately need to become adopted worldwide. The engagement activity by the Programme is therefore promoting DSbD at Government level internationally, with specific interest from the United States, Europe and Australia.

Presently we are responding to global opportunities from international stakeholders for the enablement of the broader ecosystem.

Applicability to all processor architectures

DSbD recognises the rapid change of technology and the increasing uptake of open ecosystems.

The DSbD programme has global aspirations in making the technology available to all platforms and ecosystems with a vendor agnostic ethos. To this end, RISC V becomes one of the levers to DSbD adoption by engaging and influencing the security aspects of the future roadmap for the open ISA. DSbD is working alongside Microsoft, Google and the University of Cambridge to promote, evangelise and standardise the core CHERI concepts into the RISC V community. For more information see the Microsoft tech report. [14]

How to get a board

There are multiple ways to receive a Morello Board for evaluation and participate in the DSbD ecosystem.

The technology access programme

Availability through the Digital Catapult via the Technology Access Programme (TAP). This programme has two tiers:

Tier 1 - SMEs only

- Receive funding during the course of the 6 month programme
- Receive an Arm Morello board
- Participate in one-to-one check-in sessions, practical demonstrations and focused activities for the experimentation programme
- Receive technical guidance and support from Digital Security by Design programme team
- Access Digital Catapult's labs with state-of-the art IoT and 5G network testing facilities

Tier 2 – All UK Organisations

- Receive an Arm Morello Board
- Receive technical guidance and support from Digital Security by Design programme team
- Access Digital Catapult's labs with state-of-the art IoT and 5G network testing facilities

Direct Request

For organisations who do not require the structured support that the TAP provides, direct requests can be made by both UK or international organisations.

International projects must highlight how they will develop, enrich and enhance the software ecosystem and will be handled on a case-by-case basis. Boards will be prioritised based on availability.

Why Care and Why now?

> Microsoft is one of the world's largest technology companies with products spanning the Windows operating system, personal computers, cloud platforms and services, and more. We are uniquely placed to deliver novel technology across a broad and scaled ecosystem. With this in mind, our most recent contribution to the DSbD programme has been to explore how to scale the CHERI ideas down to a tiny RISC-V microcontroller of the kind found in cheap IoT devices. Here, CHERI shows potential to gain significantly stronger security properties than anything currently available, with lower hardware complexity.
>
> *Microsoft*

There are significant challenges to deploying CHERI at scale, which the Digital Security by Design programme is intended to help address. These challenges include supporting legacy software (even if we had Morello hardware at scale today, we'd need to support non-Morello-aware binaries for 10-20 years), achieving good performance from temporal safety. However, CHERI is a disruptive technology: it enables fine-grained compartmentalisation between mutually-distrusting components and we have not yet begun to explore the space of possible new applications that this enables. Innovations with this broad a scope require support from all CPU architectures to avoid fragmenting the software ecosystem.

Memory safety errors continue to plague our industry. Our research, which provided similar results to others in the industry, suggests that they have been responsible for 70% of security vulnerabilities for over a decade. The bugs that cause these vulnerabilities are among the most dangerous because they allow the attacker to step outside the constraints that the programmer intended. This means that a single memory-safety bug can be game over for security of the affected system. CHERI breaks this first-order primitive, so that the worst that an attacker can typically do is crash the program.

This is still not ideal and safe programming languages can remove even this ability from attackers, but rewriting trillions of dollars of software in safe languages is not yet affordable. CHERI is a strong ally in the move towards safe languages. A memory-safety bug in a component of a program that is written in an unsafe language (such as C or C++) can violate all of the safety guarantees that a safe language (such as Rust, C#, or TypeScript) provided to another component. CHERI makes it possible to incrementally move parts of a program to safe languages and maintain that safety even when they're reusing large libraries of existing unsafe code.

Today, every computer from a massive cluster training a machine-learning model in Azure down to a microcontroller in a smart lightbulb is connected to the Internet. Every Internet-connected device is exposed to attackers, ranging from bored teenagers to experienced professionals backed by organised criminal organisations or rogue states. In this climate, being able to deterministically mitigate the most significant classes of vulnerabilities is not just valuable, it is essential for critical infrastructure. In addition, modern diverse software supply chains provide a lot of paths for vulnerabilities to sneak into code, either maliciously or accidentally. CHERI's memory safety does not rely on secrets or randomisation and so is strong enough to be used as a building block for isolating these components so that the blast radius of a vulnerability is limited specifically to that component and not able to damage the entire system.

Roadmap to Success

JUL 19

UK Government announce DSbD Programme

SEPT 19

Initial Collaborators Development workshops highlights opportunities

OCT 19

£37.5m Arm, University of Cambridge and University of Edinburgh project formally kicks off

JUL 20

£9.6m ESPRC research projects commence

SEPT 20

£3.5m ESRC Discribe Hub+ commences

OCT 20

Availibility of Morello Platform Model (VFP)

JAN 21

£5.8m Trance 1 Demonstrator commences

FEB / MAR 21

DSbD Four Nations roadshow

APR 21

£700k SME Ecosystem development projects kick off

JUL 21

Integrated Review of Security, Defence, Development and Foreign Policy released announcing the need to take the lead in new technologies vita to cyber power

DEC 21

UK Government announces National Cyber Strategy with a technology pillar including DSbD

JAN 22

Technology Access Programme and DSbD tech website launched

JAN 22

Arm announce Morello Board availability

JAN 22

UK Government announce government Cyber Strategy requiring government to be resillient to known vulnerabilities and attack methods by 2030

FEB 22

£9.6m Industry demonstrator projects commence

APR 22

£7.9m EPSRC and IUK Software Ecosystem Devlopment projects commence

SEPT 22

First community led conference **CHERItech22 Conference**

SEPT 22

Microsoft describe production quality implementation of a RISC V CHERI microcontroller

NOV 22

UKs Defence and Security Accelerator announce CHERI withing Defence and Security Competition

NOV 22

UKs Defence and Security Accelerator announce CHERI withing Defence and Security Competition

MAR 23

UK Industry / Government Cyber Workshop - **Security Through hardware**

APR 23

Cyber UK - Securing the foundation theme and DSbD exhibition

MAR 25

DSbD Programme ends

Anticipated commercial announcement of future Cheri tech products

Trailblazing adoption of DSbD technology solutions

Moving toward a safer, more secure future

Delivery Team and Contacts

The Digital Security by Design activity is being managed as a challenge, bringing together the specialised focus of:










Innovate UK

Innovate UK is the UK's national innovation agency supporting business led innovation.

The main DSbD delivery team sit within Innovate UK and are responsible for the day to day running of the Programme as well as the delivery of the engagement activities and the Innovate UK led competitions for industrial research.

Right: Challenge Director John Goodacre, Deputy Director Agata Samojlowicz, Senior Innovation Lead Georgios Papadakis, Programme Manager Darren Tee, Project Manager Henry Dudman, and Innovation Lead Nuala Kilmartin.

EPSRC

The Engineering and Physical Sciences Research Council provides funding for grants to undertake research and postgraduate degrees in engineering and the physical sciences.

In the DSbD Programme, EPSRC have been vital in engaging academics and administering funding for academic led research into DSbD technology.

Left: SRO Lynn Gladden, Senior Portfolio Officers Stephanie Williams & Marianne Rolph

ESRC

The Economic and Social Research Council provides funding and support for research and training in the social sciences.

The ESRC team have been integral in ensuring the funding and management of the Discribe Hub+.

Right: Senior Portfolio Officer Alice Taylor

Innovate UK KTN

The Knowledge Transfer Network exists to connect innovators with new partners and new opportunities beyond their existing thinking.

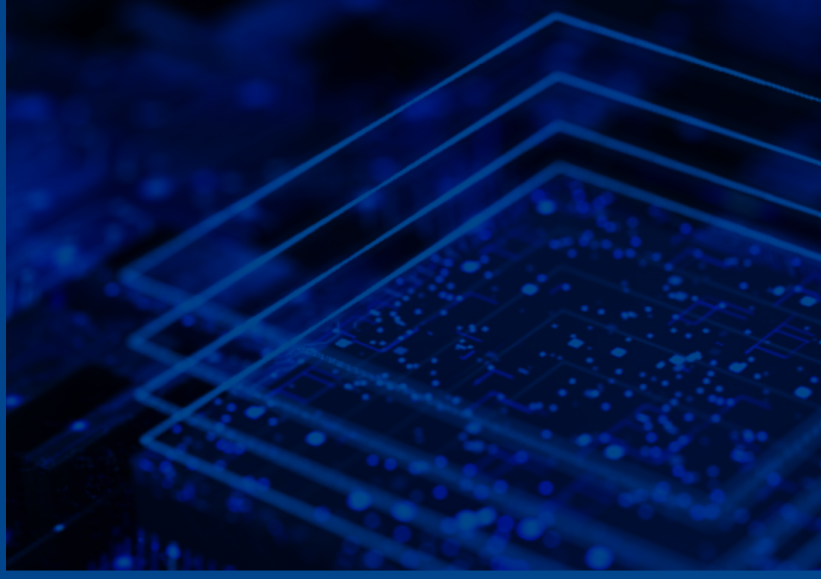
In this programme KTN have been integral at bringing together an ecosystem and ensuring the promotion of the technology and competitions.

Left: Cyber Security Lead Robin Kennedy

To get in touch with the team for more information, please contact us here

References

1. Jovanovic, Bovan. Internet of Things statistics for 2022 - Taking Things Apart Dataprot. [Online]13 May 2022. https://dataprot.net/statistics/iot-statistics.
2. Gunn, Amelia. medium.com. [Online] 3 May 2020. https://medium.com/digital-society/living-in-a-digital-world-the-causes-and-the-consequences-4c5aca11b03a.
3. Muninder, Adavelli. semiconductor-industry-statistics. https://dontdisappoint.me.uk. [Online] 3 June 2022. https://dontdisappoint.me.uk/resources/technology/semiconductor-industry-statistics/.
4. Michele Bertoncello, Christopher Martens, Timo Möller, and Tobias Schneiderbauer. Unlocking the full life-cycle value from connected-car data. McKinsey.com. [Online] 2021. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data.
5. McEnery, Sage. How much computer code has been written? Medium.com. [Online] https://medium.com/modern-stack/how-much-computer-code-has-been-written.
6. James Stannard, Rebecca Writer-Davies, Dylan Spielman, Jason Nurse. Consumer attitudes towards IoT security. London : Ipsos Mori, 2020.
7. Wright, Tim. Business Resiliency. Dell.com. [Online] 13 April 2021. https://www.dell.com/en-us/blog/how-cyber-security-is-critical-to-business-resiliency/.
8. Ransomware Recovery Cost Reaches Nearly $2 Million, More Than Doubling in a Year, Sophos Survey Shows. Sophos.com. [Online] 27 April 2021. https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.
9. Morgan, Steve. Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime magazine. [Online] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
10. DCMS. cyber-security-breaches-survey-2022. 2022.
11. Daws, Ryan. Kaspersky: Attacks on IoT devices double in a year. IoTTechNews.com. [Online] 7 September 2021. https://www.iottechnews.com/news/2021/sep/07/kaspersky-attacks-on-iot-devices-double-in-a-year/.
12. Wainwright, Matthew. https://darktrace.com/blog/the-florida-water-plant-attack-signals-a-new-era-of-digital-warfare-its-time-to-fight-back. Darktrace. [Online]
13. Hackers Remotely Kill a Jeep on the Highway—With Me in It. Wired. [Online] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
14. 14. al, Saar Amar et. CHERIoT: Rethinking security for low-cost embedded systems. [Online] Microsoft, February 2023. https://www.microsoft.com/en-us/research/publication/cheriot-rethinking-security-for-low-cost-embedded-systems/.



DSbD.tech

@DSbDTech

www.linkedin.com/company/digital-security-by-design/