UK Research and Innovation

INDUSTRIAL STRATEGY

Digital Security by Design

Securing the Future Of the Digital Economy

Vision

The Digital Security by Design (DSbD) challenge will radically update the foundation of the insecure digital computing infrastructure by creating a new, more secure hardware and software ecosystem. Built on new security capabilities, the DSbD technologies developed through this programme will underpin future digital products and services.

```
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
```

Foreword

Only once in every few generations is there an opportunity to change something as fundamental as the changes DSbD is making. Today's computer can be traced back to the designs developed in the UK during the 1940's and 50's. By as early as the 1970's, academics were documenting major issues in its design with respect to the protection and security of data. UK academic research has continued to lead the field in this area; however, the supply chain demands for software compatibility has meant we have been stuck with solutions designed without security in mind. The Arm technology developed in Cambridge UK has become the underpinning technology for most digital devices and services across the world. It is from this base that DSbD creates a programme of activities that have the opportunity to touch the lives of just about everyone in the world, without needing to change the way in which they interact with technology. This programme will ensure that the UK continues to lead both in the core technologies and the business opportunities this change will create.

John Goodacre – Challenge Director

The Challenge

The government's Industrial Strategy Challenge Fund (ISCF) brings together leading research and business to tackle the big societal and industrial challenges today.

DSbD is a wave 3 Programme from the ISCF (run by UK Research and Innovation) bringing £70m of government funding matched by £117m of industry co-investment.

Until now, the improvements that DSbD will provide have been blocked by the need to develop hardware and software simultaneously. To move both at the same time requires a revolution to the way these processes currently work rather than just an evolution of the current technology. This challenge pulls together the right strands to move the entire sector in the same direction and overcome this huge market barrier.

NCSC & Advisory Group Chair

The DSbD challenge aims to ease the burden on developers of ensuring their products are hard to exploit. Classes of software attacks which have plagued the ecosystem for decades can be mitigated in the underlying hardware. Resilient computing platforms are required to provide the confidence necessary to enable increasing uses of connected devices across the UK and around the world. Leadership in new areas of technology will demand strong foundations. This project is essential in order to lay those foundations, and to encourage development of the tools and supporting components required to make maximum use of the new protections.

Paul Waller - NCSC

National Cyber Security Centre
a part of GCHQ

Programme Objectives

This programme has three key objectives to enable the success and delivery of the vision:

1. Demonstrate a more secure hardware platform capable of protecting the integrity and resilience of software in response to significant market need for cyber security.
2. Make available the core technologies required to enable more secure platforms, for services which make extensive use of secured, personal data and create investment in new scalable businesses, digital products and services.
3. Accelerate the move towards digital transformation of industry, with the accompanying investment in productivity and improved reliability of digital services.

Programme Outcomes

The challenge aims to achieve the following:

- UK industry are motivated for change
- The UK develop new skills and jobs aligned with the new hardware and software
- Computer industry deploy new advanced security architecture
- UK to lead the world in computer security
- Increased difficulty in successful cyber attacks
- Lower costs to cyber security
- Increased research in cyber security
- Production of scalable secured products and services

For more information visit the DSbD website

Arm Dev Board

The Foundations

Technology – Capability Hardware

University of Cambridge

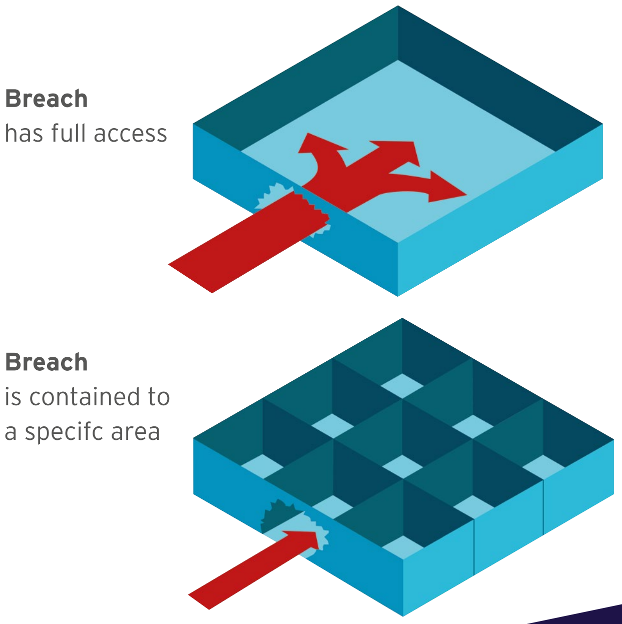
Mainstream computer systems are insecure, in large part because the conventional hardware architectures and C/C++ languages provide only coarse-grained memory protection – so coding errors become exploitable security vulnerabilities. CHERI revises the hardware/software architectural interface with hardware support for unforgeable *capabilities*, usable for fine-grained memory protection and scalable software compartmentalisation.

CHERI aims to provide practically deployable performance and compatibility, requiring only minimal changes to existing software and hardware: recompiling existing C/C++, with mild adaption, can protect pointers with capabilities. CHERI has been developed in a University of Cambridge / SRI International hardware/software/semantics co-design project since 2010. This combines hardware implementation, FPGA-based processors adapting MIPS and RISC-V; a complete software stack, adapting widely used open-source software such as Clang/LLVM, FreeBSD, FreeRTOS, and applications such as WebKit, OpenSSH, and PostgreSQL; and formal modelling and machine-checked proof of security properties of the architecture.

See https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/

All this provides strong academic validation of the ideas. We have been collaborating with Arm since 2014, and DSbD and the Morello board will create an industrial prototype, enabling the industrial evaluation that is essential to deploying CHERI in mass-market systems. This will protect all of us from a wide range of existing and future security vulnerabilities.

Compartmentalization



Technology – What is it?

Arm – Morello Programme

Morello Program one year on:
A step closer to securing our digital future

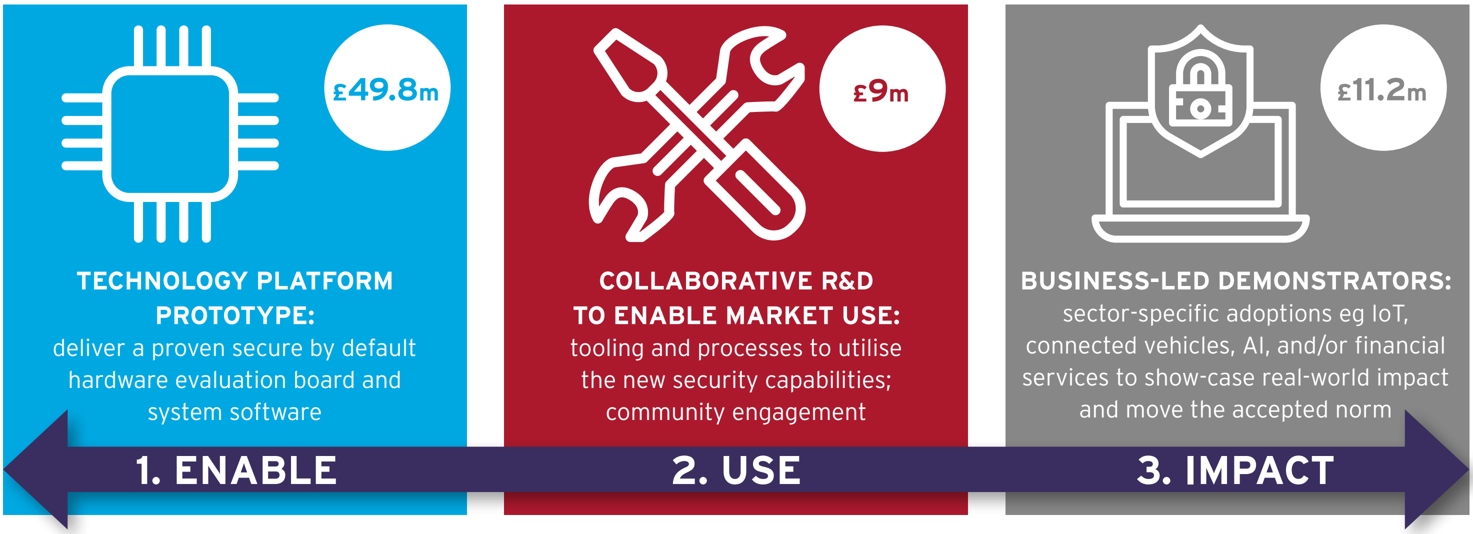
Blog Excerpt by Richard Grisenthwaite, senior vice president, chief architect and fellow at Arm – October 29, 2020

"**Releasing prototype architecture specifications: A major milestone.** When we launched this initiative, I talked about how compartmentalization works to guarantee that if there is a security breach, it will be contained within one compartment, therefore preventing the whole computing system from being compromised. Ultimately, software that is constructed with fine-grained compartmentalization could result in inherently more robust software that is resistant to attack. The Morello prototype architecture aims to improve the robustness and security of systems through the use of this scalable compartmentalization."

"**Morello Platform Model: Enabling researchers and developers to get ahead.** Prior to the launch of the Morello board (targeted for Q1, 2022), we have created a fixed virtual platform (FVP), known as the Morello platform model. The platform model uses Arm technology to create a virtual model of the system hardware, available to use in a development environment. This simulator, including the tool chain, software and documentation, will allow Morello researchers and the DSbD technology-based providers to begin writing code and running software before the prototype evaluation board comes into fruition. The Morello Platform Model is available to download from Arm's Ecosystem Platform Model Developer page."

"**Equipping the Morello community for success.** Collaboration across key partners in the Morello Program, from companies to university research teams to software developers, is critical to its success. To help this community to work openly and share key learnings, Arm is launching a support forum designed to enable ecosystem partners to ask questions, engage and help each other solve common issues. In addition, a Morello SDP Preliminary Technical Reference Manual (TRM) will also be provided, containing information about the topology and components of the Morello System Development Platform, memory, interrupt maps and register descriptions to support using the Morello Platform Model (FVP)."

Programme Activity



£49.8m

TECHNOLOGY PLATFORM PROTOTYPE: deliver a proven secure by default hardware evaluation board and system software

£9m

COLLABORATIVE R&D TO ENABLE MARKET USE: tooling and processes to utilise the new security capabilities; community engagement

£11.2m

BUSINESS-LED DEMONSTRATORS: sector-specific adoptions eg IoT, connected vehicles, AI, and/or financial services to show-case real-world impact and move the accepted norm

1. ENABLE

2. USE

3. IMPACT

Activity 1 – Enable

The DSbD team are delighted with the release of Arm's Morello prototype architecture specifications, platform model as well as Open Source Software project and tool chains which are now available to download.

This architecture introduces the principles defined in the Capability Hardware Enhanced RISC Instructions: CHERI Instruction – Set Architecture, an initiative from the University of Cambridge and SRI International.

These significant new developments mean partners now have the tools to begin participating in the program more widely which ultimately results in industrial prototype systems for secured-by-design products and services across a range of industry sectors and market applications.

Activity 2 – Use

DSbD has initiated a social science-led research programme, that will bring together social scientists, economists, computer scientists, and arts and humanities professionals for research, networking and engagement with the wider community. The DiScriBe programme will research societal challenges, cultural aspects and broader human factors underlying safety & security and privacy & trust will be undertaken to strengthen our digital systems.

This multi-disciplinary research and innovation will enable the uptake and adoption across technological, economic and societal fronts and underpin the development of new software infrastructure across the stack.

Activity 3 – Impact

With the recent engagement of The Hut Group (THG) as a business-led demonstrator, the challenge can now assess the adoption of the technology for use in ecommerce, which is the first marked demonstration area for testing.

As a cyber security demonstrator for the e-commerce industrial market, it brings key parts of a value chain to work synergistically and showcases the use of the new security capability in an industry segment(s).

This will validate its ability to underpin and deliver more secure products and services. Economic benefit and market impact will drive the business-led demonstrator activity from the very start.

Find Out More

Pathfinding

DSbD Background

National Cyber Security Centre Materials

National Cyber Security Strategy

Events/News/Videos

Programme Updates

Programme related blogs

Videos/Webinars

Technical Resources

DSbD Technical Resources

ARM Morello Project

ARM – Morello Board

Collaboration Development

Collaborators Workshop Materials

Why is DSbD Relevant?

If security is important to you, you will want to know more about how this programme is going to cause a step change in the way which computers operate.

The scope of this challenge includes implementation, verification and proof of an updated hardware architecture, development of the software and system development tools that will run on it, and demonstration in at least two industry domains.

Community Engagement

Learn about how social science and the STEM disciplines are working together to address the DSbD challenge and the regulatory and policy environment through the Digital

Security by Design Social Science Hub+ DiScriBe.

What Support is Available?

You can learn how to access government support to enable individuals and collaborative groups to peruse world class research and innovation via UK research and Innovation.

The Knowledge Transfer Network can also support partners and new opportunities to accelerate their ambitious ideas into real world

Upcoming Opportunities

Upcoming funding opportunities:

- Go to our Social Channels for News on forthcoming competitions
- Technology Enabled Business Led Demonstrator Round 2 competition opens for expressions of interest in Spring 2021

Opportunities to get involved in other ways:

- Technology platform prototype board will be available to businesses for evaluation in 2021
- Follow us on our social channels for latest updates via in @DSbDTech

www.ukri.org/innovation/industrial-strategy-challenge-fund/digital-security-by-design/

Innovate UK
Polaris House
North Star Avenue
Swindon
Wiltshire
SN2 1FL
United Kingdom

T: 01793 444000
W: ukri.org
E: support@innovateuk.ukri.org