UK Research
and Innovation

Digital Security by Design Challenge

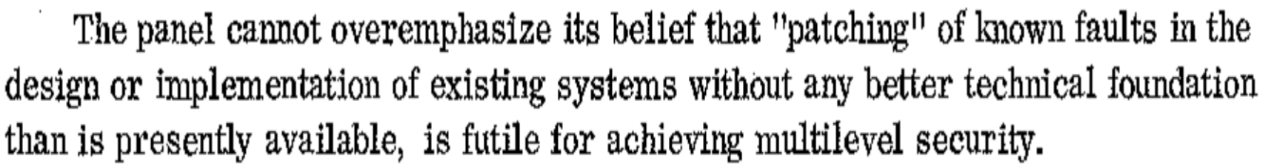
Securing the future of computing

John Goodacre

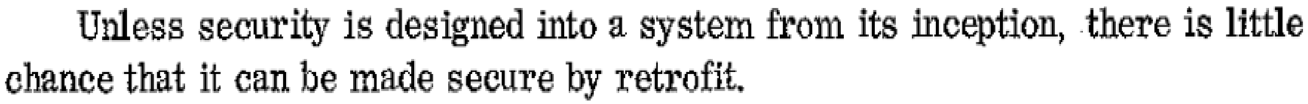
Director, Digital Security by Design
UK Research and Innovation

Prof. Computer Architectures
University of Manchester

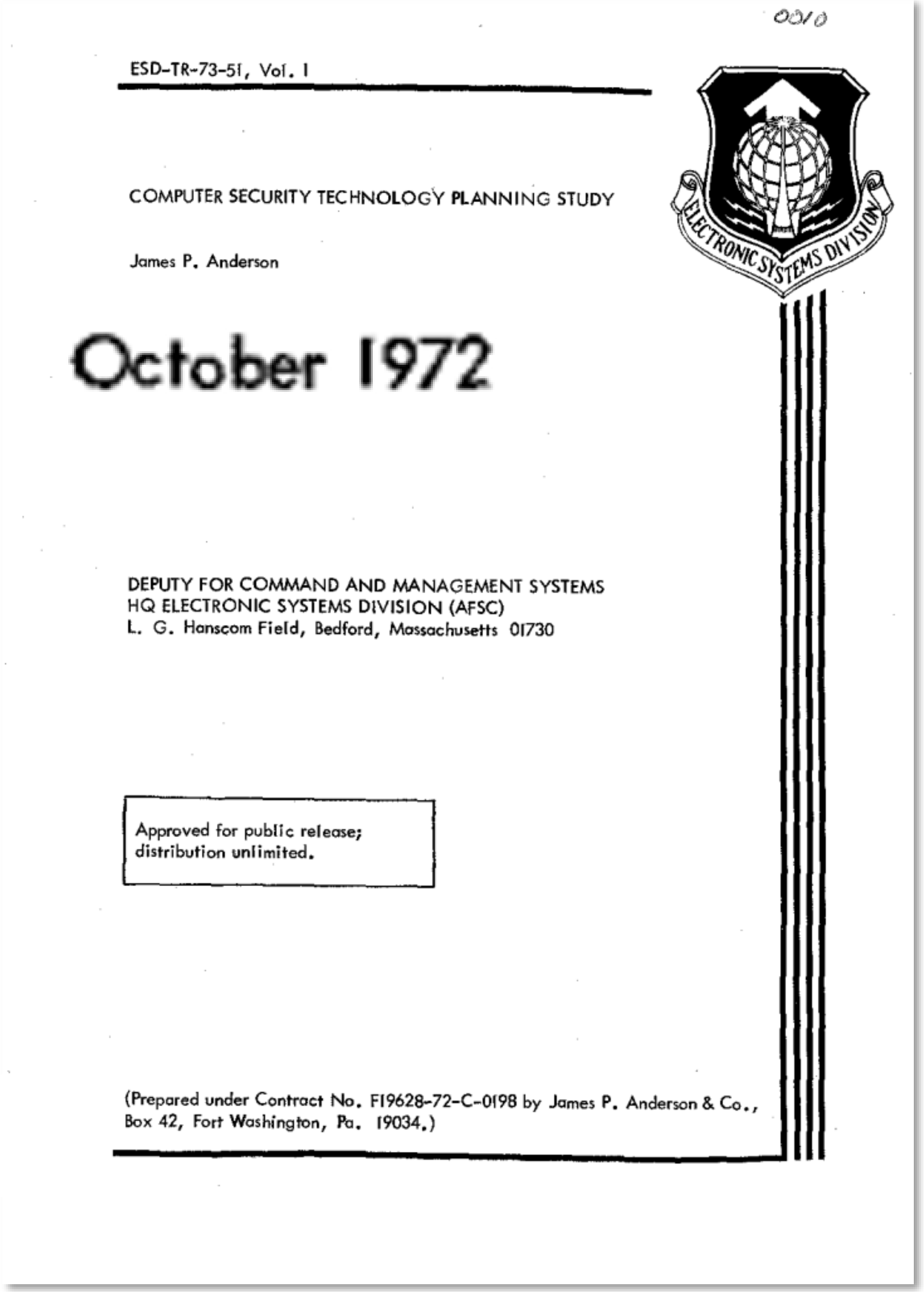
By 1972, it was becoming clear computing was broken…



The panel cannot overemphasize its belief that "patching" of known faults in the design or implementation of existing systems without any better technical foundation than is presently available, is futile for achieving multilevel security.



Unless security is designed into a system from its inception, there is little chance that it can be made secure by retrofit.



0010

ESD-TR-73-51, Vol. I

ELECTRONIC SYSTEMS DIVISION

COMPUTER SECURITY TECHNOLOGY PLANNING STUDY

James P. Anderson

October 1972

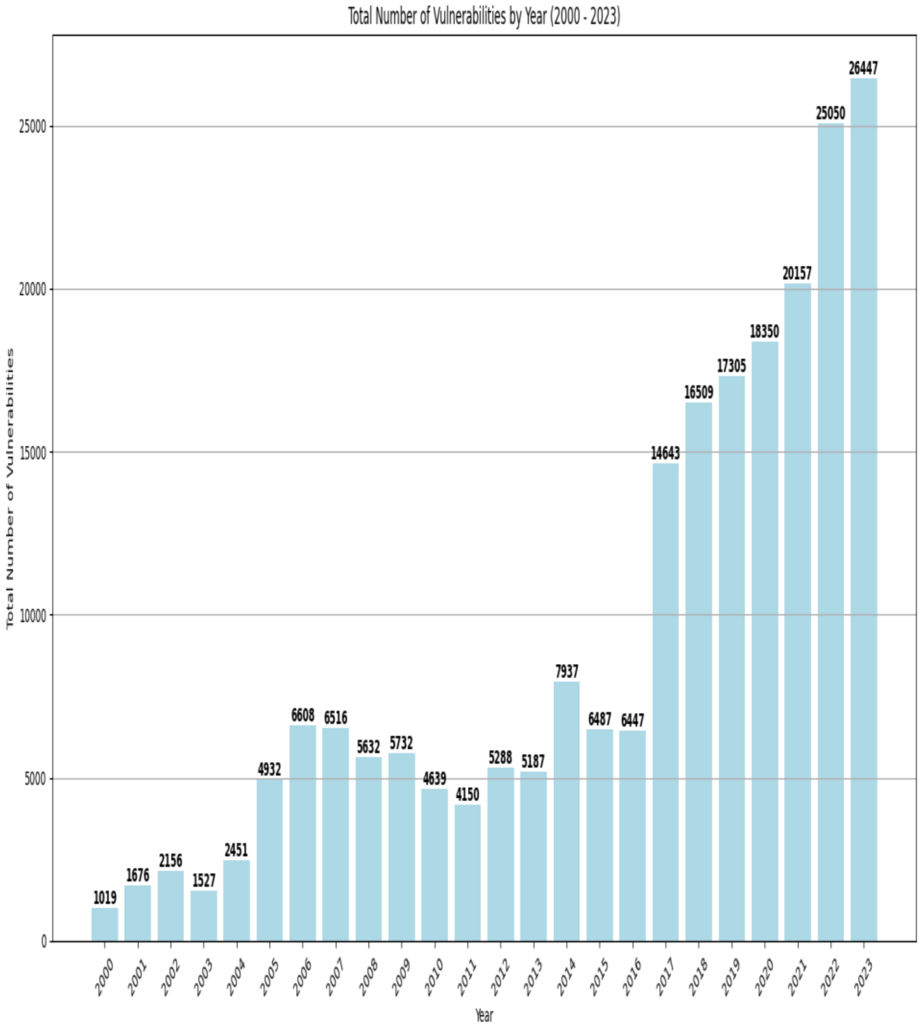
DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
HQ ELECTRONIC SYSTEMS DIVISION (AFSC)
L. G. Hanscom Field, Bedford, Massachusetts 01730

Approved for public release;
distribution unlimited.

(Prepared under Contract No. F19628-72-C-0198 by James P. Anderson & Co.,
Box 42, Fort Washington, Pa. 19034.)

https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf

Now a 50-year-old issue costing $trillions



- The global cost of cybercrime is surging.. Rising from **$9.22 trillion** in 2024 to **$13.82 trillion** by 2028

  source: statista.com

- Up to **88%** of UK companies have suffered breaches in the last 12 months

  Source: Threat Research (vmware.com)

- A small business in the UK is successfully hacked every **19 seconds**

  Source: *Hiscox Group*

- **54% of business** have acted in the past 12 months to identify a cyber security risk Source: DCMS Cyber Security Breaches Survey

- Data breaches cost UK enterprises an average of **$3.88 Million** per breach **Source:** IBM Cost of a Data Breach study.

- The average UK cybersecurity budget is around **$900,000**, compared to an average of **$1.46 million globally**

  Source: *Hiscox Group*

…by 2018 Gov/Industry aligned around ISCF…

Creating an economy that boosts productivity and earning power throughout the UK

Our five foundations

Ideas
the world's most innovative economy

People
good jobs and greater earning power for all

Infrastructure

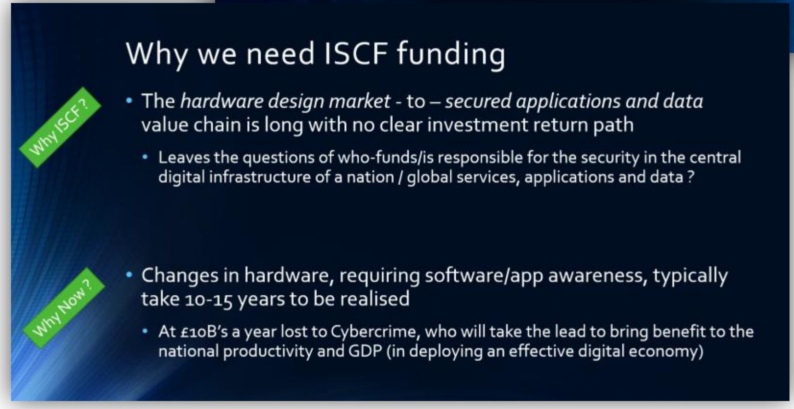
AI & Data Economy
We will put the UK at the forefront of the artificial intelligence and data revolution

Future of Mobility
We will become a world leader in the way people, goods and services move

UK Research and Innovation

Securing the Future

ESTABLISHING A TRUSTWORTHY DIGITAL INFTRASTRUCTURE FOR INDUSTRY, GOVERNMENT AND SOCIETY

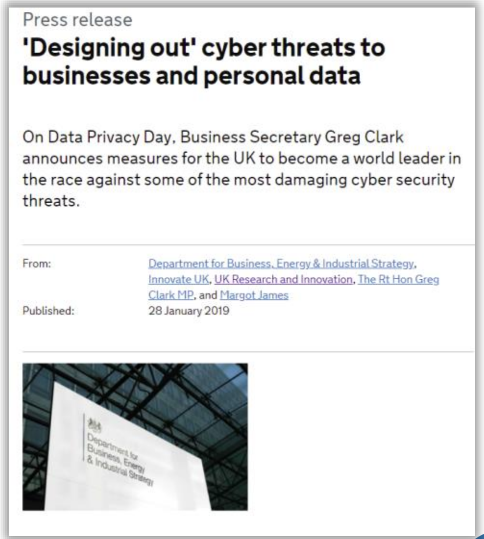


Why we need ISCF funding

Why ISCF?
Why Now?

- The *hardware design market* - to – *secured applications and data* value chain is long with no clear investment return path
  - Leaves the questions of who-funds/is responsible for the security in the central digital infrastructure of a nation / global services, applications and data ?
- Changes in hardware, requiring software/app awareness, typically take 10-15 years to be realised
  - At £10B's a year lost to Cybercrime, who will take the lead to bring benefit to the national productivity and GDP (in deploying an effective digital economy)

- 2018: UKRI asked UK industry "what are your challenges ISCF could help solve?
- They described a failure in market dynamics that was stopping industry from introducing new technology that could block vulnerabilities from exploit
- Some UK research output looked like it could help
- Funding announced Jan 2019
  - Programme designed in collaboration



Press release

'Designing out' cyber threats to businesses and personal data

On Data Privacy Day, Business Secretary Greg Clark announces measures for the UK to become a world leader in the race against some of the most damaging cyber security threats.

From: Department for Business, Energy & Industrial Strategy, Innovate UK, UK Research and Innovation, The Rt Hon Greg Clark MP, and Margot James
Published: 28 January 2019

ISCF DSbD Challenge Vision

(at start of programme)

By 2025, the ISCF Digital Security by Design challenge aims to **overcome the market failures** and **radically update the foundation of the insecure digital computing infrastructure** that underpins the entire economy. A new and secure computer hardware approach, proven in at least two major industrial markets, will protect against at least half of known and associated future technological vulnerabilities

Working up for the first time from the central hardware of a digital device

DSbD, an initiative supported by the UK government to transform digital technology and create a resilient, and secure foundation for a safer future.

Programme as a "Facilitator"

Digital Security by Design

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

- **Objective**: DSbD was to address fundamental security issues in current digital infrastructure by developing by-design focused secure hardware and software ecosystem.
- **Collaboration**: The programme involves collaboration between academia, industry, and government, including partners like DSIT, NCSC, MoD, Arm, University of Cambridge, Google, and Microsoft.
- **Technologies**: DSbD focuses on creating new security capabilities that limit the impact of vulnerabilities by-design and ensure only expected access to data and operations.
- **Prototype Hardware**: The programme has developed the Morello and Sonata board that implements the CHERI protection model for fine-grained memory protection and scalable software compartmentalization.
- **Community Engagement**: Developers and tech organizations can access prototype hardware and software, participate in networking events, and contribute to open-source projects.
- **Funding and Support**: The DSbD Technology Access Programme provides technical guidance, prototype hardware, and funding for eligible companies to experiment with DSbD technologies.

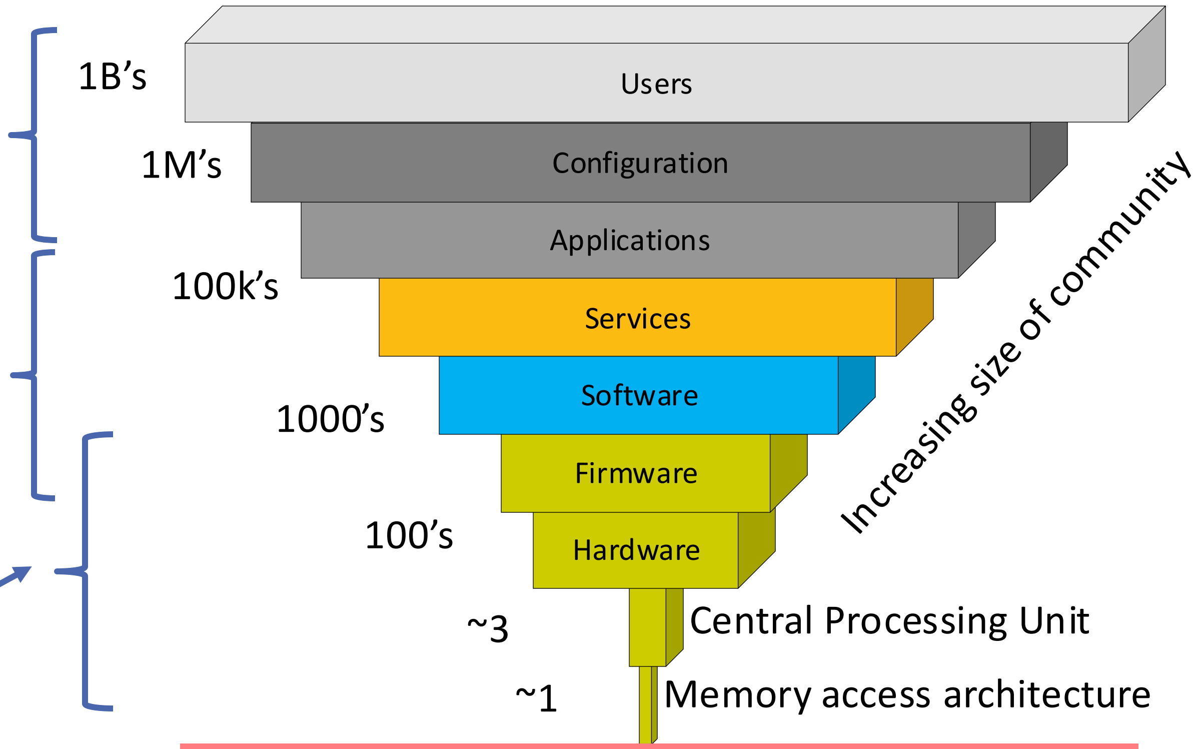
Why could a (small) UK Programme “change the world”

Cybersecurity is focused on configuration management, best practices, monitoring and patching

Software manufacturers must deliver more secure services and applications **by default**

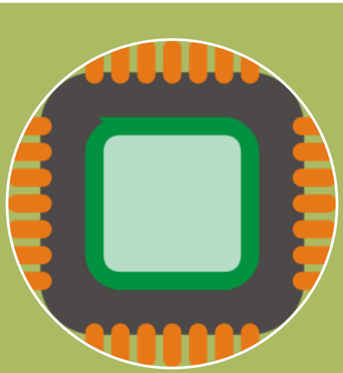
But still, hardware and related components need to protect against software vulnerabilities **by design**

The Cyber Pyramid



NOTE: The entire digital economy and infrastructure are balanced on architectures that are fundamentally vulnerable to the exploitation of any mistakes in software implementation or design

DSbD's Delivery Approach



Enabling Technology

Prototype Platform

Deliver a proven secure-by-default hardware evaluation board and
system software

Technology Sector

Collaborative R&D

To enable market use, tooling and processes to utilise the new security capabilities; ecosystem enablement

Industry Sector

Business-led Demonstrators and Technology Access Programme

Sector defined applications showcase impact and move the accepted norm

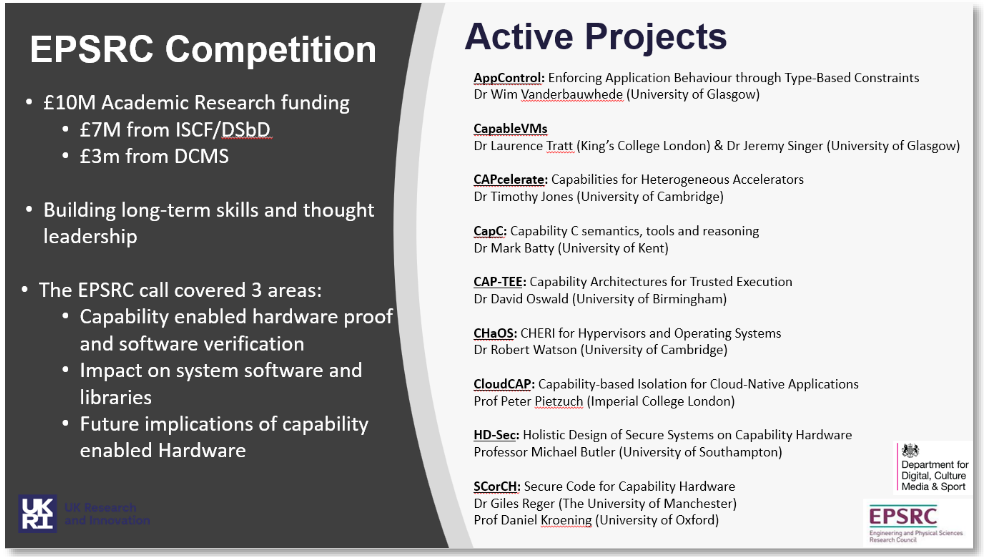
1. DSbD Enablers

2. Technology Developers

3. End Markets

Building of an inclusive ecosystem:

Academic Focused



EPSRC Competition

- £10M Academic Research funding
  - £7M from ISCF/DSbD
  - £3m from DCMS
- Building long-term skills and thought leadership
- The EPSRC call covered 3 areas:
  - Capability enabled hardware proof and software verification
  - Impact on system software and libraries
  - Future implications of capability enabled Hardware

Active Projects

AppControl: Enforcing Application Behaviour through Type-Based Constraints
Dr Wim Vanderbauwhede (University of Glasgow)

CapableVMs
Dr Laurence Tratt (King's College London) & Dr Jeremy Singer (University of Glasgow)

CAPcelerate: Capabilities for Heterogeneous Accelerators
Dr Timothy Jones (University of Cambridge)

CapC: Capability C semantics, tools and reasoning
Dr Mark Batty (University of Kent)

CAP-TEE: Capability Architectures for Trusted Execution
Dr David Oswald (University of Birmingham)

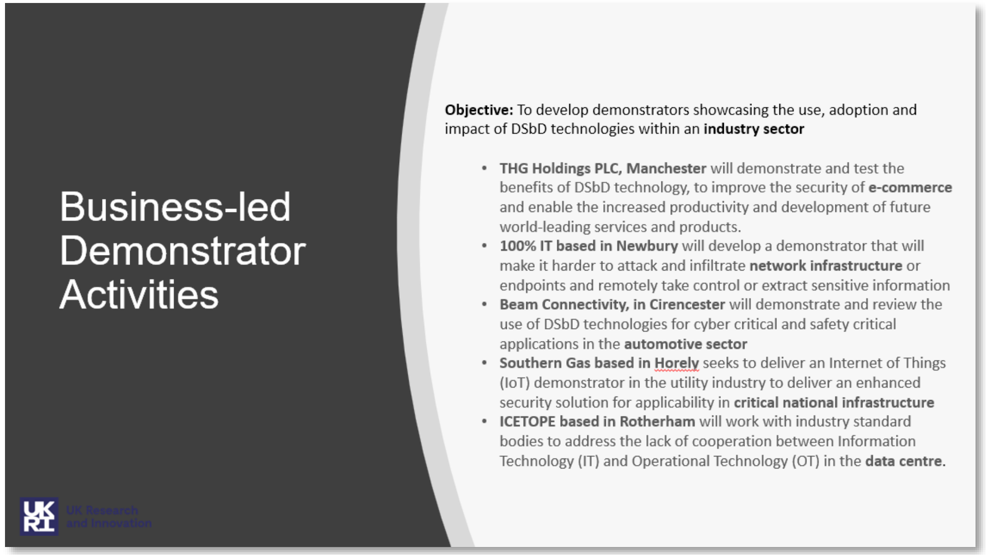
CHaOS: CHERI for Hypervisors and Operating Systems
Dr Robert Watson (University of Cambridge)

CloudCAP: Capability-based Isolation for Cloud-Native Applications
Prof Peter Pietzuch (Imperial College London)

HD-Sec: Holistic Design of Secure Systems on Capability Hardware
Professor Michael Butler (University of Southampton)

SCorCH: Secure Code for Capability Hardware
Dr Giles Reger (The University of Manchester)
Prof Daniel Kroening (University of Oxford)

Business Led

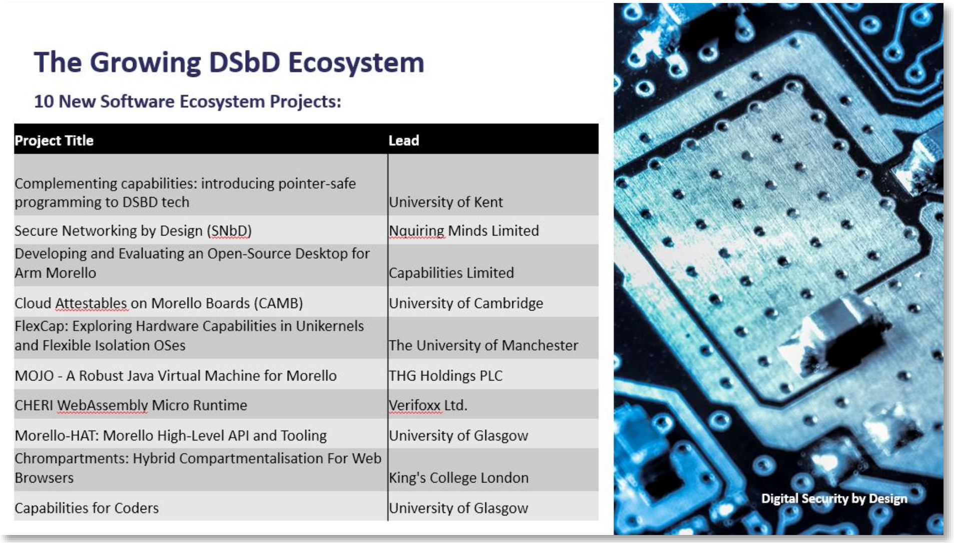


Business-led Demonstrator Activities

Objective: To develop demonstrators showcasing the use, adoption and impact of DSbD technologies within an **industry sector**

- **THG Holdings PLC, Manchester** will demonstrate and test the benefits of DSbD technology, to improve the security of **e-commerce** and enable the increased productivity and development of future world-leading services and products.
- **100% IT based in Newbury** will develop a demonstrator that will make it harder to attack and infiltrate **network infrastructure** or endpoints and remotely take control or extract sensitive information
- **Beam Connectivity, in Cirencester** will demonstrate and review the use of DSbD technologies for cyber critical and safety critical applications in the **automotive sector**
- **Southern Gas based in Horely** seeks to deliver an Internet of Things (IoT) demonstrator in the utility industry to deliver an enhanced security solution for applicability in **critical national infrastructure**
- **ICETOPE based in Rotherham** will work with industry standard bodies to address the lack of cooperation between Information Technology (IT) and Operational Technology (OT) in the **data centre.**

Technology Driven



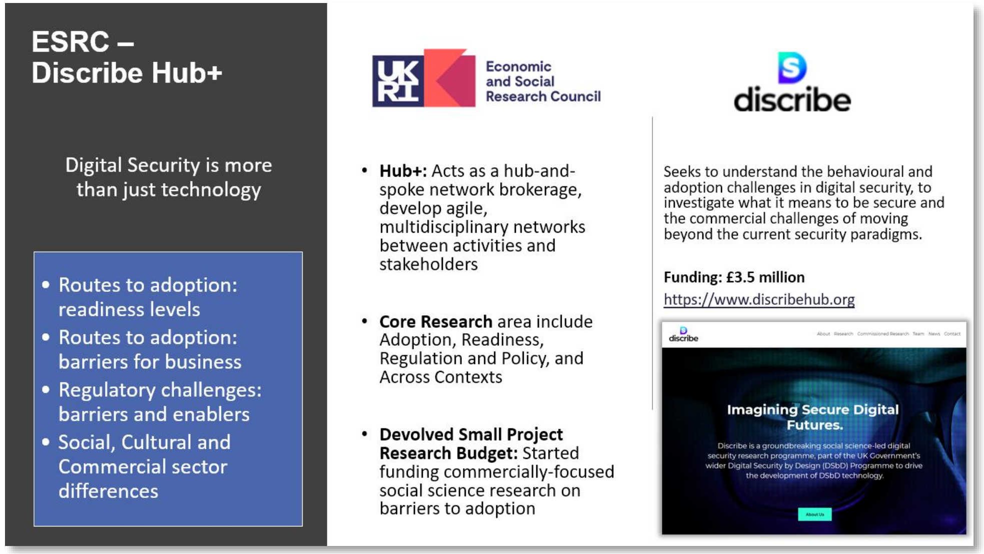
The Growing DSbD Ecosystem

10 New Software Ecosystem Projects:

Project Title	Lead
Complementing capabilities: introducing pointer-safe programming to DSBD tech	University of Kent
Secure Networking by Design (SNbD)	Nquiring Minds Limited
Developing and Evaluating an Open-Source Desktop for Arm Morello	Capabilities Limited
Cloud Attestables on Morello Boards (CAMB)	University of Cambridge
FlexCap: Exploring Hardware Capabilities in Unikernels and Flexible Isolation OSes	The University of Manchester
MOJO - A Robust Java Virtual Machine for Morello	THG Holdings PLC
CHERI WebAssembly Micro Runtime	Verifoxx Ltd.
Morello-HAT: Morello High-Level API and Tooling	University of Glasgow
Chrompartments: Hybrid Compartmentalisation For Web Browsers	King's College London
Capabilities for Coders	University of Glasgow

Digital Security by Design

Social & Economic



ESRC – Discribe Hub+

Digital Security is more than just technology

- Routes to adoption: readiness levels
- Routes to adoption: barriers for business
- Regulatory challenges: barriers and enablers
- Social, Cultural and Commercial sector differences

- **Hub+:** Acts as a hub-and-spoke network brokerage, develop agile, multidisciplinary networks between activities and stakeholders
- **Core Research** area include Adoption, Readiness, Regulation and Policy, and Across Contexts
- **Devolved Small Project Research Budget:** Started funding commercially-focused social science research on barriers to adoption

Seeks to understand the behavioural and adoption challenges in digital security, to investigate what it means to be secure and the commercial challenges of moving beyond the current security paradigms.

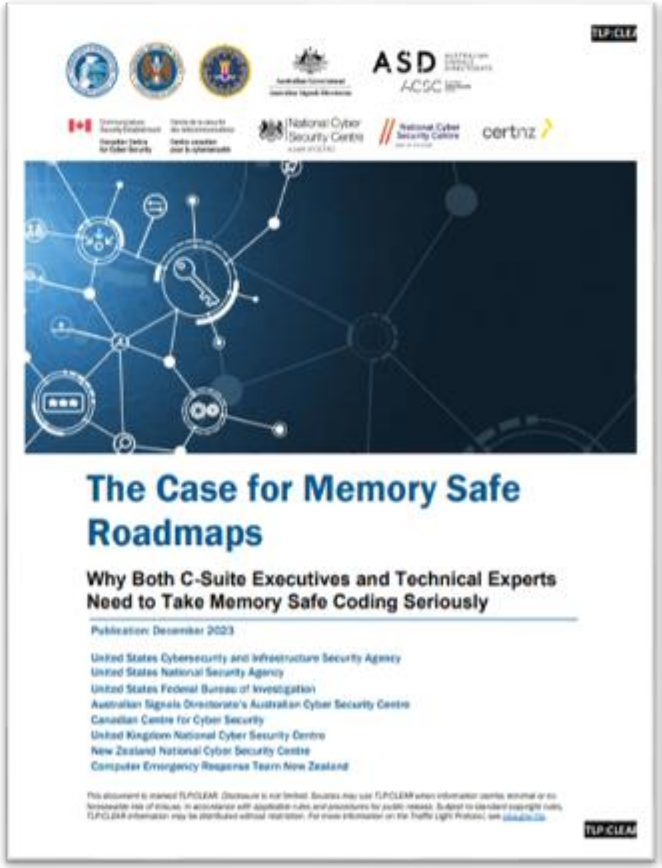
Funding: £3.5 million
https://www.discribehub.org

Imagining Secure Digital Futures.

Discribe is a groundbreaking social science-led digital security research programme, part of the UK Government's wider Digital Security by Design (DSbD) Programme to drive the development of DSbD technology.

Now part of Governments’ Strategy

Delivered by Innovate UK, EPSRC and ESRC



TLP:CLEAR

ASD ACSC

certnz

The Case for Memory Safe Roadmaps

Why Both C-Suite Executives and Technical Experts Need to Take Memory Safe Coding Seriously

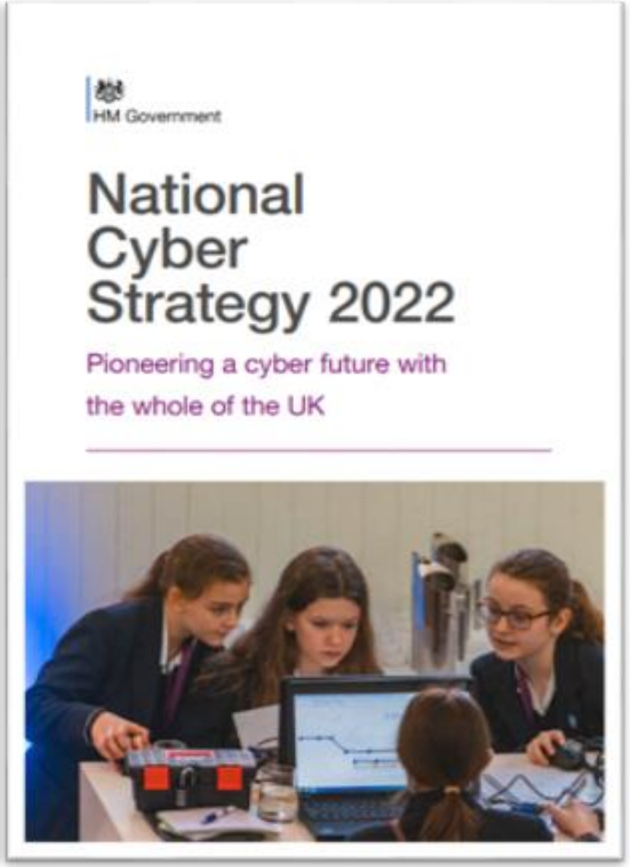
Publication: December 2023

United States Cybersecurity and Infrastructure Security Agency
United States National Security Agency
United States Federal Bureau of Investigation
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
United Kingdom National Cyber Security Centre
New Zealand National Cyber Security Centre
Computer Emergency Response Team New Zealand

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

17 International Cyber Agencies: Case for Memory Safety

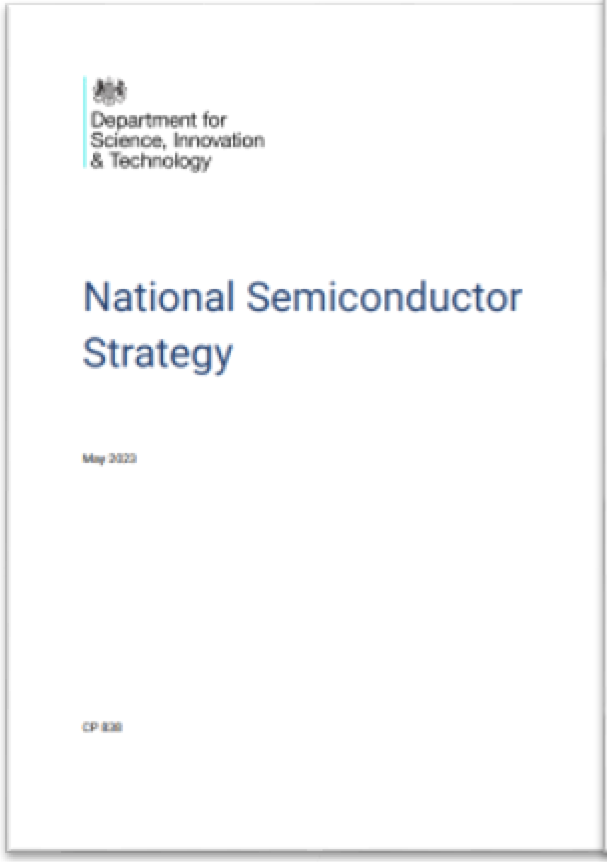


HM Government

National Cyber Strategy 2022

Pioneering a cyber future with the whole of the UK

UK National Cyber Strategy: Technology Pillar



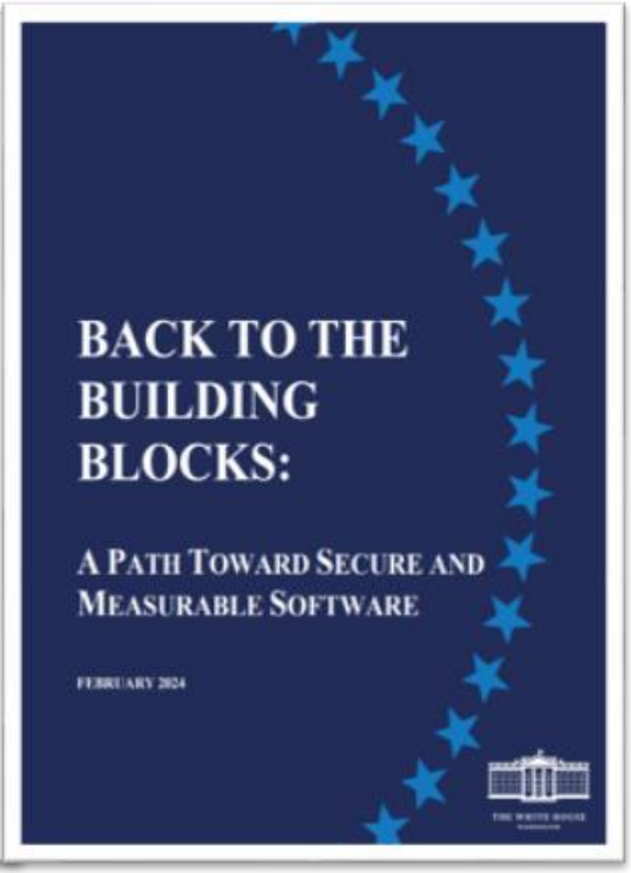
Department for Science, Innovation & Technology

National Semiconductor Strategy

May 2023

CP 838

UK Semiconductor Strategy



BACK TO THE BUILDING BLOCKS:

A PATH TOWARD SECURE AND MEASURABLE SOFTWARE

FEBRUARY 2024

THE WHITE HOUSE

USA’s Whitehouse Technical Report

Summary at Programme End

Demonstratable broken the targeted market failure

Showing approach can block around 70% of ongoing vulnerabilities and associated costs

Matured required technologies ready for commercial adoption and deployment

Part of international/gov language and strategy

Now investigating guidance / policy / procurement etc

Increasing alignment of international response and posture to cyber-risks and mitigations

International ecosystem that is cross discipline/sector/ market / gov / academic / business / etc

Organizations have formed "CHERI Alliance" to align on standards and enablement

Over 200 enterprise software organization signed up to "Secure by Design Pledge"

New business and large business departments created to deploy and commercialise

Various RISC-V devices and IP

Being design-in most "root of trust" devices by big-tech businesses

Still work required to achieve ubiquitous deployment (post programme goal)

Increased international awareness and collaboration

"Helping" tech supply chain understand their responsibility

Making the end-customers know more can be done

UK Research and Innovation

Thank you!

John Goodacre
Prof. Computer Architectures
University of Manchester

Director, Digital Security by Design
UK Research and Innovation