

Systems & Software Security (S3)

The University of Manchester

Verifiable, trustworthy software and secure networked systems; capability, engagement routes and talent, for BT Group

Prof. Lucas C. Cordeiro

Professor of Computer Science · Area Lead, Systems & Software Security

Director, Arm Centre of Excellence · Department of Computer Science

lucas.cordeiro@manchester.ac.uk

Business engagement event · 9 September 2026 · The University of Manchester

Six things, thirty minutes

Who S3 is

13 academics,
six areas

What BT has said

in BT's own
published words

Where the two overlap

our reading
of the fit

What we have built

tools,
competitions,
adoption

Talent

who we teach
and supervise

How to start

four concrete
first projects

Systems & Software Security at Manchester

“We develop state-of-the-art algorithms, methods and protocols to address security and privacy in networked and distributed system environments, and tools to build verifiable, trustworthy software and AI/ML systems.”

The University of Manchester is one of 21 universities jointly recognised by the NCSC and EPSRC as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR)

13 academics

Lucas Cordeiro
(Area Lead)

Richard Banach

Alex Creswell

Daniel Dresner

Boris Fouotsa

Sebastian Köhler

Bernardo Magri

Edoardo Manino

Mustafa Mustafa

Gaven Smith

Zhipeng Wang

Dominik Winterer

Ning Zhang

A national cyber-security research centre with a systems and software security core

Six research areas

1
Cryptography

2
**Networked, distributed
and cyber-physical
systems security**

3
**Data and identity
privacy**

4
**Systems and Software
Verification**

5
**Systemic view of
governance in cyber
resilience**

6
AI safety and security

Cryptography through code assurance through governance; one group, one corridor.

BT's six stated research areas

Converged “Build a converged network for a seamless customer experience”

Sustainable “Build an optimised network that's sustainable”

Platform “Build a network that's a platform”

Future “Build a network for future technologies”

Secure “Build a network that's secure against emerging threats”

Quantum ready “Build a network for quantum technologies”

Quantum-secure, sovereign, and AI-assisted

Quantum

“...we are developing quantum-secure networks using technologies like PQC, Quantum Key Distribution (QKD) and entanglement-based security...”

“...the launch of the Quantum-Secure Metro Network (QSMN) in London. Developed by BT in partnership with Toshiba, it uses QKD to protect data moving between businesses.”

Sovereign

“As digital resilience becomes a growing priority, for UK organisations we have launched a sovereign services platform, bringing together connectivity, voice, cloud and AI services.”

*BT Annual Report 2026
(summary), for the year ended
March 2026.*

AI-assisted engineering

“BT's engineering teams are using AI-assisted development tools to automate repetitive work like coding, testing, and modernising legacy systems.”

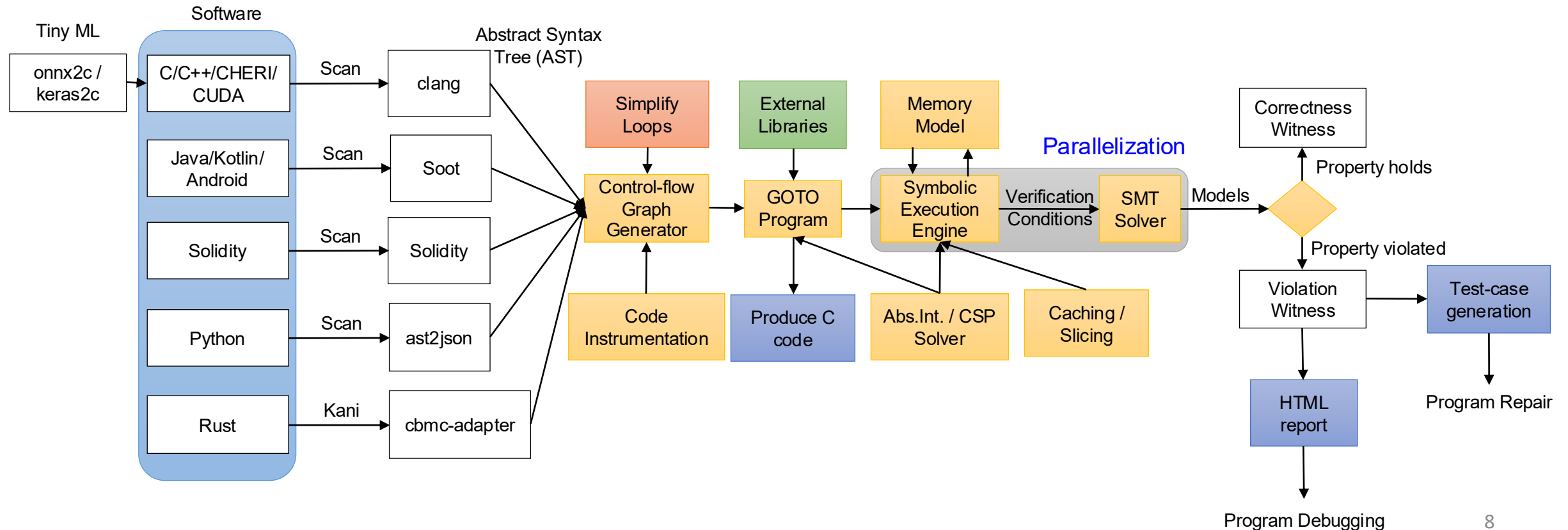
*BT Annual Report 2026
(summary), for the year ended
March 2026.*

Our reading of the fit

BT stated research area	S3 research area	Who
Secure, network secure against emerging threats	Systems and Software Verification	Cordeiro, Winterer, Manino
Secure, network secure against emerging threats	Networked and distributed system / CPS security	Zhang, Köhler, Mustafa
Quantum ready, network for quantum technologies	Cryptography	Fouotsa, Wang, Magri
AI-assisted engineering	AI safety and security	Manino, Cordeiro

ESBMC, proving the absence of runtime errors

“ESBMC (the Efficient SMT-based Context-Bounded Model Checker) is a mature, permissively licensed open-source context-bounded model checker that automatically detects or proves the absence of runtime errors in single- and multi-threaded C, C++, CUDA, CHERI, Kotlin, Python, Rust, and Solidity programs.”



Judged by competition, not by press release

56

medals from SV-COMP and
Test-Comp, 2012–2026,
Cordeiro's career total
across ESBMC, JBMC and
FuSeBMC

SV-COMP 2026

JBMC placed first (gold) in
Java.Overall, ahead of GDart and
JLiSA; Cordeiro is a JBMC co-author
ESBMC-kind placed second (silver) in
C.ReachSafety, behind CPAchecker,
ahead of Symbiotic

Test-Comp 2026

FuSeBMC placed first in C.Overall,
C.Cover-Error and C.Cover-Branches

Annual, blind, third-party benchmarking; the same evidence any competitor would be judged on.

Six open-source codebases under the checker

Not benchmarks. Production code from AWS, NVIDIA, Google and vLLM, verified with ESBMC during 2026. Every claim below is a public artefact: a CVE, a merged PR, or a maintainer's comment.

AWS SDK for C++

Base64 decoder, DateTime parsers, HexDecode.

Two out-of-bounds defects, CVE-2026-19642 and CVE-2026-19643, fixed in 1.11.862; two integer overflows in PR #3896.

NVIDIA OpenSMA

22 modules of C++ server-management firmware.

Out-of-bounds array write reachable from one MCTP packet, proven from network input. NVIDIA confirmed and fixed it.

vLLM

Config validation and KV-cache integer arithmetic.

Eight findings — CLI flags that pass every validator, then crash the engine. Five fixed upstream (PRs #43794, #44070, #44207).

Chromium Dashboard

Google's Chrome feature-tracking API backend.

Ten input-validation findings; three fixed with our patch. Two security invariants came back proven.

AWS Neuron NKI

Accelerator kernels for Trainium and Inferentia.

Shape and bounds contracts checked on every kernel call, without a NeuronCore. Two division-by-zero defects fixed upstream.

boto3

AWS SDK for Python: collections, DynamoDB expressions.

Three findings confirmed against the real library, each with an executable pytest reproduction. Filed as boto/boto3 #4831.

Six upstream projects, two published CVEs, and fixes merged by AWS, NVIDIA and Google maintainers.

What came back from the maintainers

2

CVEs in the AWS C++ SDK
Base64 decoder, fixed in
1.11.862

15

of 18 reported defects fixed
upstream by AWS, NVIDIA,
Google and vLLM

240

public, re-runnable
harnesses across six
repositories

57

issues filed against ESBMC
itself, most now fixed

Worked example: CVE-2026-19642 and CVE-2026-19643

ESBMC returned two concrete inputs to `Aws::Utils::Base64::Base64::Decode`, the decoder every AWS C++ service response passes through: one wrote past the end of the output buffer, one read past the end of the input. Reported 29 July 2026, published 12 August, fixed in 1.11.862.

AND WHERE THERE WAS NO BUG, A PROOF

A Chromium Dashboard gate cannot be approved without the votes it requires, three for a three-reviewer gate, never two. OpenSMA's DCD GPIO handlers stay in bounds (536 verification conditions), each paired with a broken control ESBMC catches.

Absence of a bug is a result too, but only when the checker is shown to catch the bug you planted.

Accepted into the Rust standard library verification effort

On 7 August 2025 the Rust Foundation announced *“the successful integration of a new formal verification tool, ESBMC (Efficient SMT-based Context-Bounded Model Checker), into the Rust standard library verification initiative”*

“The currently accepted tools are Flux, GOTO Transcoder (ESBMC), Kani, and VeriFast.”

Flux

**GOTO Transcoder
(ESBMC)**

Kani

VeriFast

Who verifies the verifier?

Dominik Winterer joined Manchester in September 2025 as Lecturer in Cyber Security and leads the Formal Methods Engineering Lab. He directed a bug-hunting effort that uncovered over 1,800 bugs and enabled more than 1,300 fixes in SMT solvers

One of four tools accepted to verify the Rust standard library, and the researcher behind one of academia's largest SMT-solver bug-hunting campaigns now leads our lab.

If AI writes more of the code, something has to check it

BT's position, quoted: "BT's engineering teams are using AI-assisted development tools to automate repetitive work like coding, testing, and modernising legacy systems."

AI WRITES → C · C++ · Python · Rust · Kotlin · Solidity



VERIFIER CHECKS → ESBMC reads all of those languages

OUR INTERPRETATION

The same checker therefore applies to generated code in several of the languages a modern network estate is written in. We have not measured this on BT's codebase.

Edoardo Manino is Lecturer in AI Security in S3 and works on automated verification of neural networks

| A £1.7m EPSRC programme on guarding neural architectures, and a checker that reads the languages the code comes out in.

Running the benchmark, not just entering it

25

benchmarks in the VNN-COMP 2025 suite, 16 in the regular track, 9 in the extended

Manchester runs the track

Edoardo Manino is Benchmark Chair for VNN-COMP 2025 and 2026, running the submission and voting process that fixes what every entrant's tool is tested on, and co-authoring the official results report.

How the benchmarks are chosen

Proposed by the community, then voted into the regular track by the tool entrants themselves. Networks in ONNX, specifications in VNN-LIB, every tool on equal-cost AWS hardware.

A gentle introduction

AAAI-26 Lab LH03 on VNN-COMP, for benchmark proposers, tool entrants and the broader AI community, co-organised by Manino, Singapore, January 2026.

Funded to do this work

Manino is PI on Hardware-Level AI-Safety Verification, ARIA funded, £496,798, October 2025, February 2027, with Birmingham.

The group that runs the benchmark track sees what every one of these tools can and cannot do.

Post-quantum, in the group, now

BT: “...we are developing quantum-secure networks using technologies like PQC, Quantum Key Distribution (QKD) and entanglement-based security...” · QSMN launched in London with Toshiba

October 2024

NIST announces 14 candidates advancing to round 2 of the Additional Digital Signatures process, SQIsign among them

January 2026

Tako Boris Fouotsa joins S3 as Lecturer in Cryptography; post-quantum isogeny-based cryptography; contributor to SQIsign

May 2026

NIST IR 8610 advances nine candidates to round 3 of the Additional Digital Signatures process, SQIsign among them

Zhipeng Wang, Lecturer in Cyber Security

“applied cryptography, including classical and post-quantum solutions”; also “security, privacy, and trust in collaborative and agentic AI systems”

Bernardo Magri, Senior Lecturer

Subversion-resilient cryptography, foundations of blockchain, key exchange, cryptography from noisy sources, secure multi-party computation

BT is building quantum-secure networks; we hired a SQIsign contributor, SQIsign being a NIST third-round signature scheme, in January.

Security below the application

Sebastian Köhler

Lecturer in Cyber Security

“wireless and physical-layer security of Cyber-Physical Systems, spanning space and satellite systems, smart grids, and autonomous and electric vehicles”

research.manchester.ac.uk/en/persons/sebastian-kohler/

Ning Zhang

Senior Lecturer

“security in networked and distributed systems, applied cryptography, data privacy, trust and digital right managements”; 29 PhD students supervised to completion per her profile, with at least one further completion in 2025

research.manchester.ac.uk/en/persons/ning-zhang-2/

Mustafa A. Mustafa

Senior Lecturer

Security and privacy in smart grids, smart metering and peer-to-peer electricity trading and applied cryptography; deputy director of the Centre for Digital Trust and Society and of the ACE-CSR

research.manchester.ac.uk/en/persons/mustafa-mustafa

Wireless, distributed-systems and critical-infrastructure security, alongside the code-level work.

Selected grants

Programme	Reference	Role and dates	Value
EnnCore: End-to-End Conceptual Guarding of Neural Architectures	EP/T026995/1	Manchester lead; PI Lucas Cordeiro; Feb 2021 – Dec 2025 (completed)	£1,721,559
SCorCH: Secure Code for Capability Hardware	EP/V000497/1	Manchester lead; PIs Konstantin Korovin and Giles Reger; Pierre Olivier, Mustafa Mustafa and Lucas Cordeiro co-investigators; ISCF; Jun 2020 – Mar 2025 (completed)	£1,034,989
SECCOM: Securing composable hardware platforms	EP/X037290/1	Manchester lead; PI John Goodacre; Bernardo Magri and Lucas Cordeiro co-investigators; status Active; 1 Sep 2023 – 31 Aug 2026	£789,633
Hardware-Level AI-Safety Verification	MSAI-SE01-P004	Manchester lead; PI Edoardo Manino; Mirco Giacobbe co-investigator (University of Birmingham); ARIA funded; Oct 2025 – Feb 2027	£496,798

Beyond these examples, Prof. Cordeiro's career totals: over USD 16.4M in research funding; more than 190 peer-reviewed publications, h-index 36; 14 PhD theses, three MPhil and 35 MSc dissertations supervised

Funders include Amazon, BAE Systems, British Council, CNPq, EPSRC, the European Commission, FAPEAM, GCHQ, Innovate UK, Intel, Motorola, Nokia Institute of Technology, the Royal Society, Samsung and UKRI

Who we teach, and who we supervise

What S3 teaches

The group contributes teaching to the MSc Cyber Security, whose compulsory units are Introduction to Cryptography; Network Security; Secure Computer Architecture and Systems; Security and Privacy in Artificial Intelligence; Formal Methods for Software Verification, Security and Computer Science; and Software Security.

Doctoral supervision

Ning Zhang has supervised 29 PhD students to completion, per her profile
13 academics supervise across cryptography, verification, networks, privacy, governance and AI security

The national context

One of 21 NCSC/EPSRC-recognised Academic Centres of Excellence in Cyber Security Research
ACE-CSR co-directed by Daniel Dresner and Mustafa Mustafa, both S3 members

OUR INTERPRETATION

Career engagement routes we can offer: industry-set MSc project topics, co-supervised industrial PhDs, placements and internships, guest lectures and technical talks.

A supervision and teaching pipeline in exactly the subjects the security roles are hard to fill in.

The mechanisms, yours and ours

BT already runs the route

“Through our partnership programme we collaborate with over thirty top universities as well as start-ups, scale-ups, investors... and publicly funded bodies such as UKRI.”

“We work with around 150 partner organisations as part of our Collaborative Research Programme.”

What Manchester brings to it

Multi-partner, multi-year delivery: EnnCore, SCorCH, SECCOM — £3.5M combined

An established industry–university centre: the Arm Centre of Excellence, directed by Lucas Cordeiro
National recognition as an ACE-CSR

Funded by industry

Arm, Intel, Amazon, BAE Systems, Motorola and the Ethereum Foundation

Run on production code

Two CVEs in the AWS SDK for C++ (CVE-2026-19642/3), found with ESBMC and fixed upstream

Taken to market

VeriBee and ByteRepair, two University of Manchester spinouts

The four starting projects on the next slide are sized to fit any one of BT's existing partnership routes.

We are not asking BT to invent a route; we are asking to enter one that exists.

Four concrete first projects

A

Code assurance pilot

Who Cordeiro, Winterer

What Run ESBMC over one BT-nominated C/C++/Rust/Python component

You get back Counterexamples with concrete inputs, or a proof

Basis Permissive licence, no procurement blocker

How long *to be agreed*

B

Post-quantum readiness review

Who Fouotsa, Wang, Magri

What Review one signature or key-establishment use case against NIST's additional-signatures track

You get back A written readiness assessment

Basis BT's stated PQC priority

How long *to be agreed*

C

Assurance for AI-assisted development

Who Manino, Cordeiro

What A scoped study on checking AI-generated code in one BT toolchain

You get back A method and a measured baseline on your own code

Basis BT's stated use of AI-assisted tools

How long *to be agreed*

D

Security of Device-2-Device communication

Who Köhler

What Security review of D2D cellular links against physical-layer threats

You get back A written evaluation of the D2D attack surface

Basis Growing deployment of D2D services

How long *to be discussed*

Each is a weeks-to-months piece of work with a named academic and a checkable outcome.

What we are asking for

1

A 30-minute technical follow-up

with whoever owns software assurance in the network estate

2

One nominated component

for pilot A, the code assurance pilot

3

A named BT contact

for the Collaborative Research Programme route

And, for the careers side of this event: industry-set MSc project topics, co-supervised industrial PhDs, placements and guest lectures; say which is useful and we will scope it.

The cheapest possible next step.

Contact

Prof. Lucas C. Cordeiro

Professor of Computer Science

Area Lead, Systems & Software Security

Director, Arm Centre of Excellence

lucas.cordeiro@manchester.ac.uk

cs.manchester.ac.uk/research/expertise/systems-and-software-security/