Systems and Software Security (S3)

Develop methods, algorithms, and tools to safeguard data and communication

Lucas Cordeiro
Department of Computer Science
lucas.cordeiro@manchester.ac.uk

Research Team
(11 members)

L. Cordeiro   R. Banach   M. Mustafa   N. Zhang   D. Dresner   B. Magri

K. Korovin   G. Reger   C. Kotselidis   M. Luján   A. Creswell

Research Objective

We develop state-of-the-art algorithms, methods, and protocols to address **security** and **privacy** in **distributed and embedded systems** and tools to build verifiable, **trustworthy software systems**

Research Areas

- **Cryptography:** develop the theoretical and practical aspects of techniques to secure digital information, transactions and distributed computations

- **Blockchain:** develop foundational aspects and applications for permissionless and permissioned blockchain systems

- **Distributed and embedded system security:** design security solutions for intelligent systems (crypto, protocols and architectures)

- **Data and identity privacy:** design, analyse and implement privacy-enhancing technologies
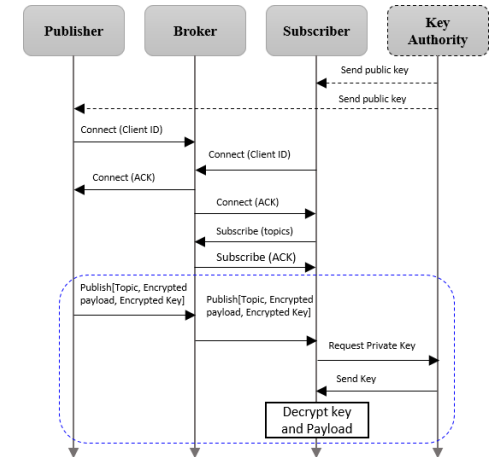
Research Areas

- **Systems and software verification:** develop algorithms and tools to mathematically demonstrate correctness, safety, and security of software systems

- **Systemic view of governance in cyber resilience:** We learn from the limited integration of historic sociotechnical approaches to the tacit based on situational awareness and forensic readiness to enable them to cope with attacks and other failures
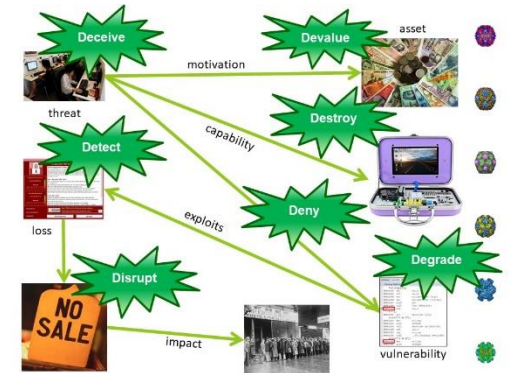
IASME: A Spin off in Cyber-Security

- ISAME (https://iasme.co.uk/) is the only comprehensive information and cyber security benchmark dedicated to SMEs

Information Assurance for Small to Medium-Sized Enterprises

Award-Winning Software

- Develop award-winning **theorem provers** and **software verifiers** to ensure safe and secure HW/SW systems:
    - Vampire and iProver
    - ESBMC, JBMC and FuSeBMC
    - MAMBO
- Contributions to **software verification** and **automated reasoning**: build **trustworthy software systems**
- We have strong links to the industry, including collaborations with ARM, Intel, Microsoft, AWS, NASA, and THG

Teaching in Cyber-Security

- **MSc in Computer Security** 2020/2021:

  - Cryptography

  - Cyber Security

  - Systems Governance

  - Software Security

- **NCSC Certification** of an MSc with Cyber Security

- **MSc in Cyber-Security** 2022/2023:

  - Network Security

  - Ethical Hacking

Research Grants (~GBP 7M)

- UKRI project [Soteria: demonstrating the security capabilities of the Morello System in the e-commerce vertical industrial segment](#) - over the call for ISCF digital security by design: technology-enabled business-led demonstrator

- EU project [ELEGANT: secure and seamless edge-to-cloud analytics](#) - over the call for software technologies

- EPSRC project [SCorCH: secure code for capability hardware](#) - over the call for ISCF digital security by Design Research Projects

- EPSRC project [EnnCore: end-to-end conceptual guarding of neural architectures](#) - over the call for security for all in an AI-enabled society

- ERDF 15R18P02426 [Greater Manchester Cyber Foundry](#)

Centre for Digital Trust and Society

Centre for Digital Trust and Society

A focal point for research across the University that explores aspects of trust and security in our digital world.

Find out more ›

Clusters

Digital Technologies and Crime

Focuses on analysing and understanding criminal activity across the digital spectrum.

Trusted Digital Systems

Developing tools, policies and practices to safeguard data and communication.

Workplace and Organisational Security

Researching institutional security, insider threats, supply chain security and psychology of crime.

Democracy and Trust

Researching the threats that digital technologies and AI pose to trust and security in democratic systems.

Privacy and Trust

Focusing on the interplay of a complex number of topics around privacy and confidentiality.

Advanced Mathematics

Applying advanced mathematical theory and methods for cyber security.