Trustworthy Systems Group

Developing and deploying real-world systems with unprecedented assurance quickly and effectively

Expertise

World leaders in the intersection of Formal Methods and Systems Software

Applications

Cyber security and high-assurance software systems

seL4

Software Systems

Formal Proofs

Programming Languages & Information Flow

Concurrency & Distributed Systems

DARPA HACMS

CDDC

Micro VM

Cogent
Trustworthy Systems Group Expertise

**Software Systems**

- **Trustworthy secure operating system kernels**
- **Componentised architecture and applications**

**Operating System Kernel**

- Microkernel design and development (seL4, L4::embedded)
- Mixed-criticality real-time systems
- Information flow and side channels
- Real-time operating systems for constrained devices (eChronos)
- Linux kernel

**Componentised applications**

- Secure software architectures
  - High-assurance systems software design and development
  - Using verified isolation properties
- Componentised systems
  - Microkernel and capability-based systems (seL4 and L4-family)
  - Component platform development (CAmKES)
- System Components
  - Device drivers
  - File systems, network stacks
  - Virtual machines

Small, fast, capability-based operating system kernel
“World’s most verified kernel”
Open Source: [http://seL4.systems](http://seL4.systems)
Trustworthy Systems Group Expertise

Formal Proofs

- Mathematical guarantee of correctness & security
- Proof engineering to make it scale

Software verification

- World leading in large-scale formal verification of software systems
- Formal reasoning about security and information flow
- Mathematical, machine-checked proofs from spec to the binary code

Proof Engineering

Proof production at a large scale

- Estimating proof effort
- Continuous Integration
- Increasing proof Automation
- Proof Refactoring

Refinement proof from high-level spec to binary
On-going ports to new platforms
Trustworthy Systems Group Expertise

Programming Languages & Information Flow

Functional programming and type systems
Domain specific languages, e.g. for formal file system verification
Compiler verification, e.g. Cogent systems language; CakeML
Programming language semantics and implementation, e.g. MicroVM

Information Flow

• Security critical properties verified of real software
• World leading in formal reasoning about information flow, leakage and side-channels, with applications in eVoting and operating systems (seL4)

CakeML

• World first realistic verified compiler for full functional programming language
• End-to-end verification: from syntax to machine code
• Tools for development of high assurance software in CakeML, including functional correctness verification
Trustworthy Systems Group Expertise

Concurrency & Distributed Systems → Formal reasoning about concurrency

- Modelling and verification of systems
- Foundational research in concurrency
- Applications range from operating system (OS) to protocols

Wireless mesh protocols

Communication protocols

Information leakage and voting

Interruptible Embedded OS

Multicore kernel

- Applications
  - task A
  - task B
  - handler 1
  - handler 2
  - handler 3

Interrupt handlers

- OS
  - signal_send
  - signal_wait
  - mutex_lock
  - mutex_unlock
  - scheduler

- core
- core
- core

- memory

- NSA
- G
- CIA

- S
- G
- CIA

- (0)
- (2)
Aim
- Protecting autonomous vehicles from cyber attacks

What
- Air vehicles: quadcopter, Boeing optionally-piloted helicopter
- Ground vehicles: robot, autonomous army trucks

How
- Using high-assurance software development techniques
- Formalised architecture
- Synthesised code
- Verified isolation (seL4 and CAmkES)

Results
- Vehicles running high-assurance software
- Resist attacks by Red Team

Mission Computer

Flight Computer

Ground Station Link

WiFi

Camera

Sensors

Motors
Problem

Cross domain solutions are critical for government and business productivity. Current solutions offer very poor usability (e.g. secure KVM switch) or have known insecure foundations (e.g. Xen).

Insight

Combine DST Group secure hardware compositing with Data61’s verified software control and configuration to produce a solution that simultaneously maximises both usability and security.

Impact

A new synergy for building verified, secure cross domain systems. The CDDC is currently planned for trial on Defence networks in 2017.
Trustworthy Systems Group Project

Micro VM

Trustworthy platform for managed language applications

Problem

Important programming languages suffer very poor performance and/or inscrutable semantics (e.g., PHP, Python, and JavaScript).

Insight

Extreme engineering challenges at the heart of languages lead to poor language design decisions, resulting in systemic poor performance and unreasonable semantics. A thin substrate addressing these liberates language designers & implementers.

Impact

New opportunities for future language design on a mature and verified substrate.
New capabilities and better performance for existing languages.
Working with PyPy and Haskell developers.

Collaborators
Data61
ANU
Purdue U.
U. Mass.

Resources
http://microvm.org

Micro VM solves very hard problems that lie here.
Cogent

Reducing the costs of system verification

Code and proof Co-generation

Manual verification doesn’t scale for systems components like file systems, where we need many different implementations.

Cogent is a formally specified, fast, purely functional, high-level language, without garbage collection.

Cogent compiler emits C code, as well as a correctness proof for the generated code.

It significantly reduces verification effort by automising boiler plate proofs and providing convenient interface for remaining manual proof.