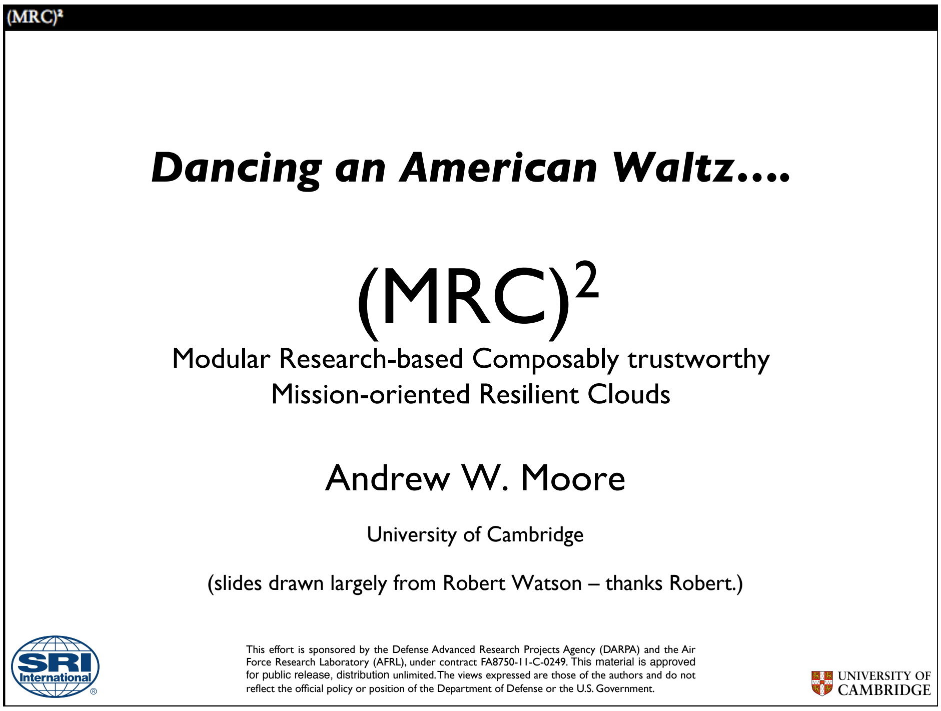


(MRC)^2

Dancing an American Waltz....

(MRC)^2

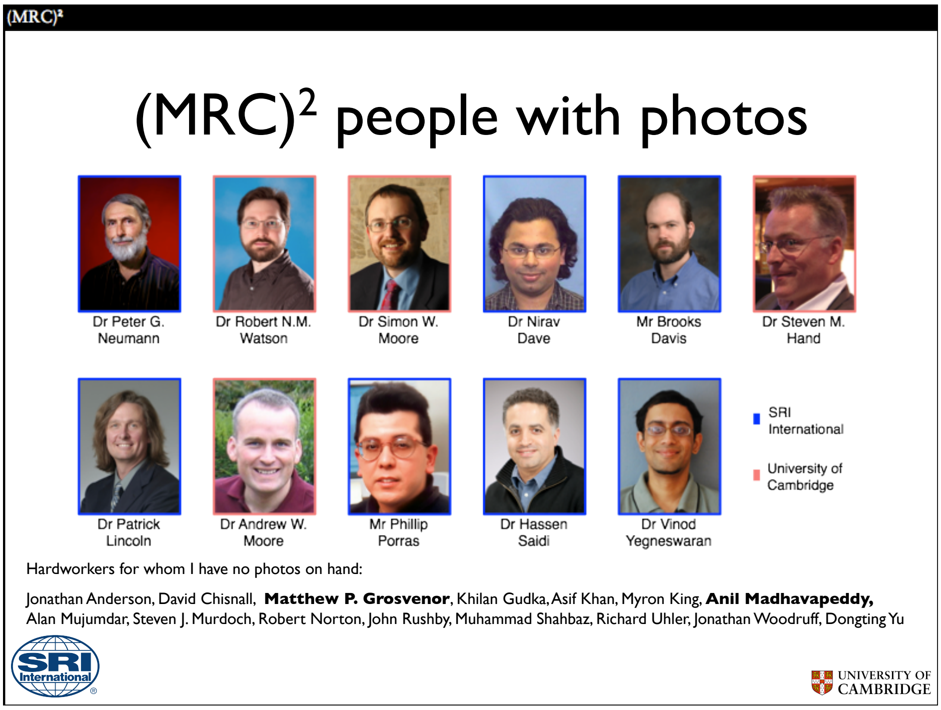
Modular Research-based Composably trustworthy
Mission-oriented Resilient Clouds

Andrew W. Moore

University of Cambridge

(slides drawn largely from Robert Watson – thanks Robert.)

This effort is sponsored by the Defense Advanced Research Projects Agency (DARPA) and the Air Force Research Laboratory (AFRL), under contract FA8750-11-C-0249. This material is approved for public release, distribution unlimited. The views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.



(MRC)^2

(MRC)^2 people with photos

Dr Peter G. Neumann

Dr Robert N.M. Watson

Dr Simon W. Moore

Dr Nirav Dave

Mr Brooks Davis

Dr Steven M. Hand

Dr Patrick Lincoln

Dr Andrew W. Moore

Mr Phillip Porras

Dr Hassen Saidi

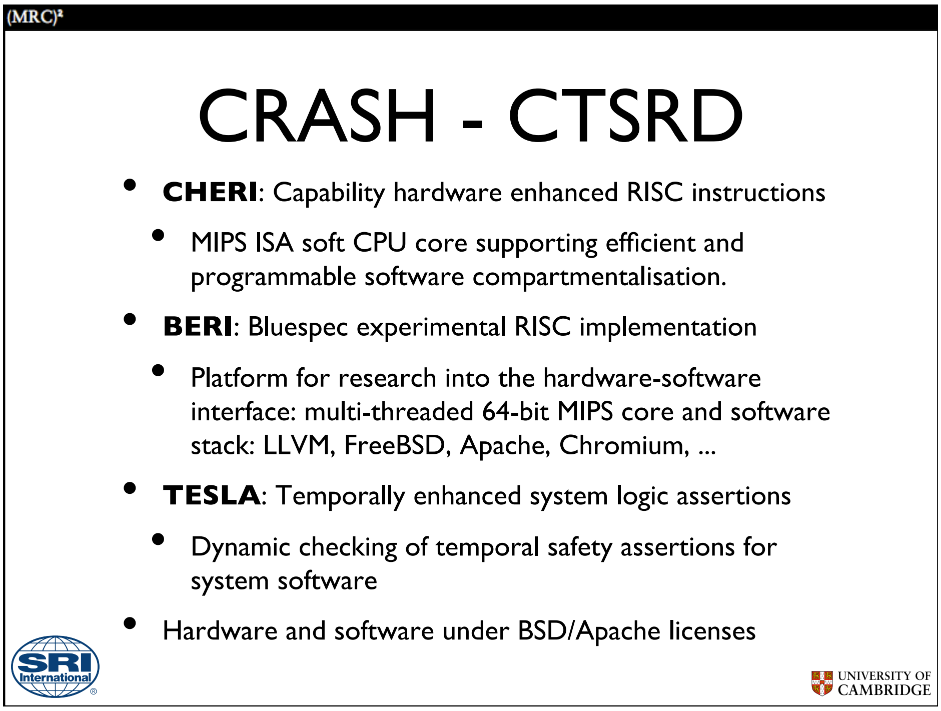
Dr Vinod Yegneswaran

🟦 SRI International

🟥 University of Cambridge

Hardworkers for whom I have no photos on hand:

Jonathan Anderson, David Chisnall, **Matthew P. Grosvenor**, Khilan Gudka, Asif Khan, Myron King, **Anil Madhavapeddy,** Alan Mujumdar, Steven J. Murdoch, Robert Norton, John Rushby, Muhammad Shahbaz, Richard Uhler, Jonathan Woodruff, Dongting Yu



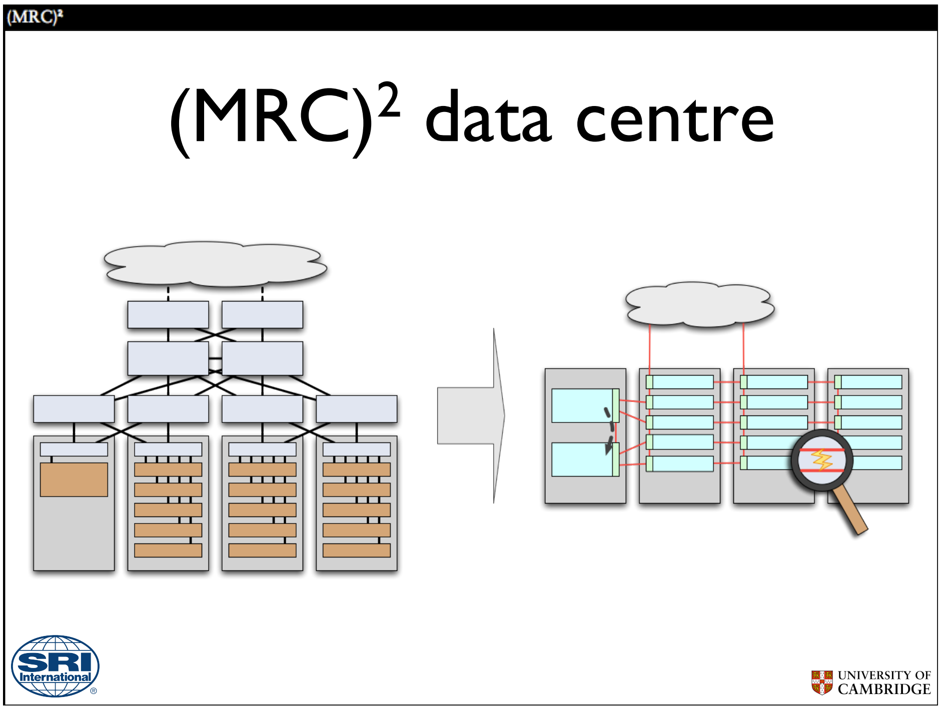
(MRC)²

CRASH - CTSRD

- **CHERI**: Capability hardware enhanced RISC instructions
  - MIPS ISA soft CPU core supporting efficient and programmable software compartmentalisation.
- **BERI**: Bluespec experimental RISC implementation
  - Platform for research into the hardware-software interface: multi-threaded 64-bit MIPS core and software stack: LLVM, FreeBSD, Apache, Chromium, ...
- **TESLA**: Temporally enhanced system logic assertions
  - Dynamic checking of temporal safety assertions for system software
- Hardware and software under BSD/Apache licenses

SRI International

UNIVERSITY OF CAMBRIDGE



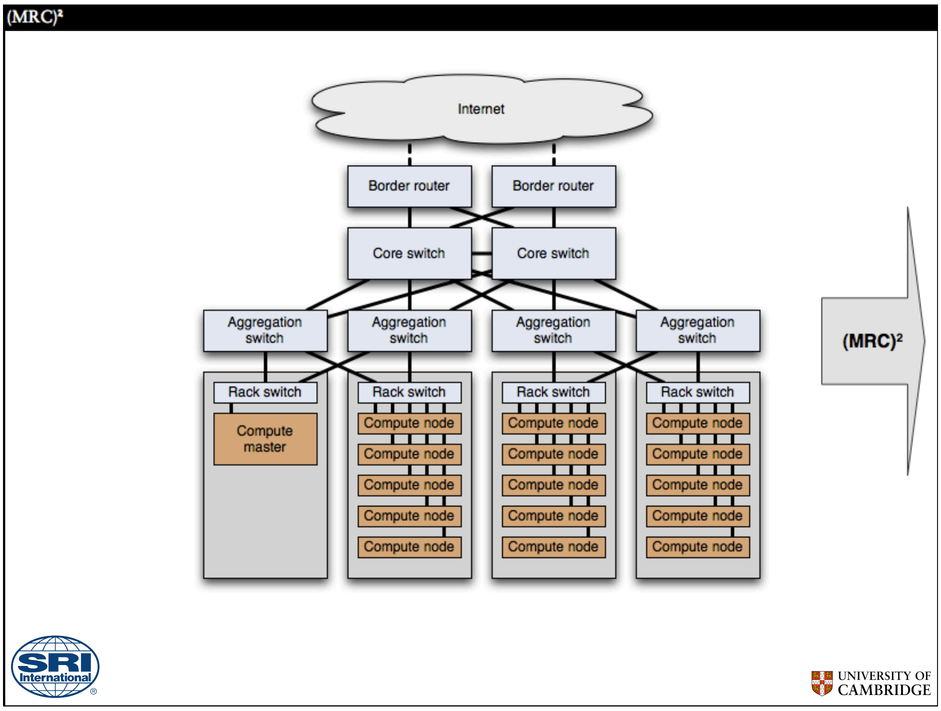
(MRC)²

$(\mathrm{MRC})^2$ data centre

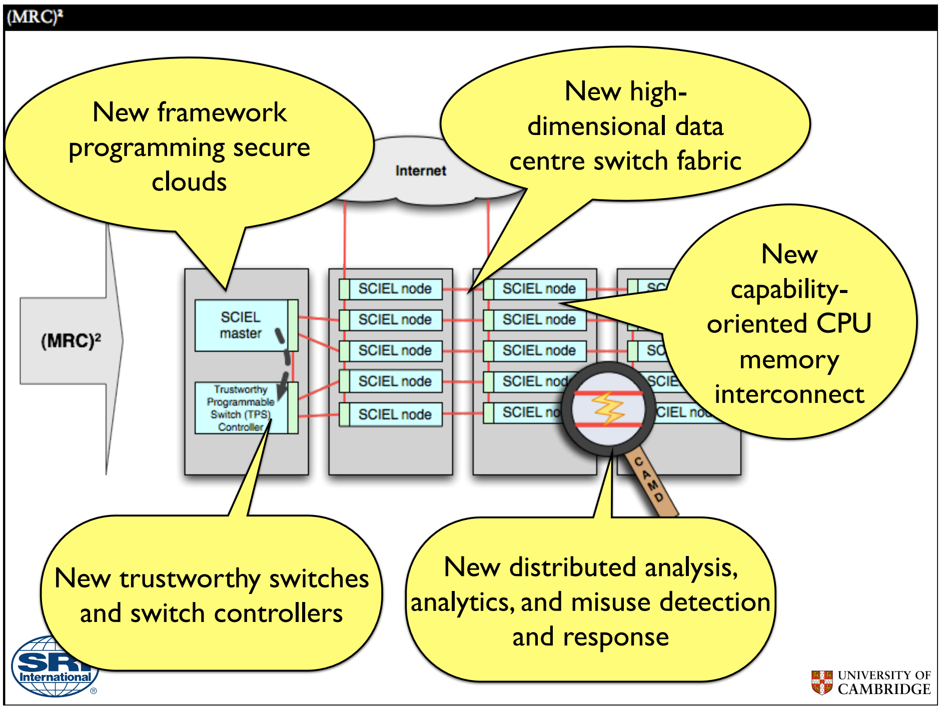
SRI International

UNIVERSITY OF CAMBRIDGE

(MRC)²



(MRC)²



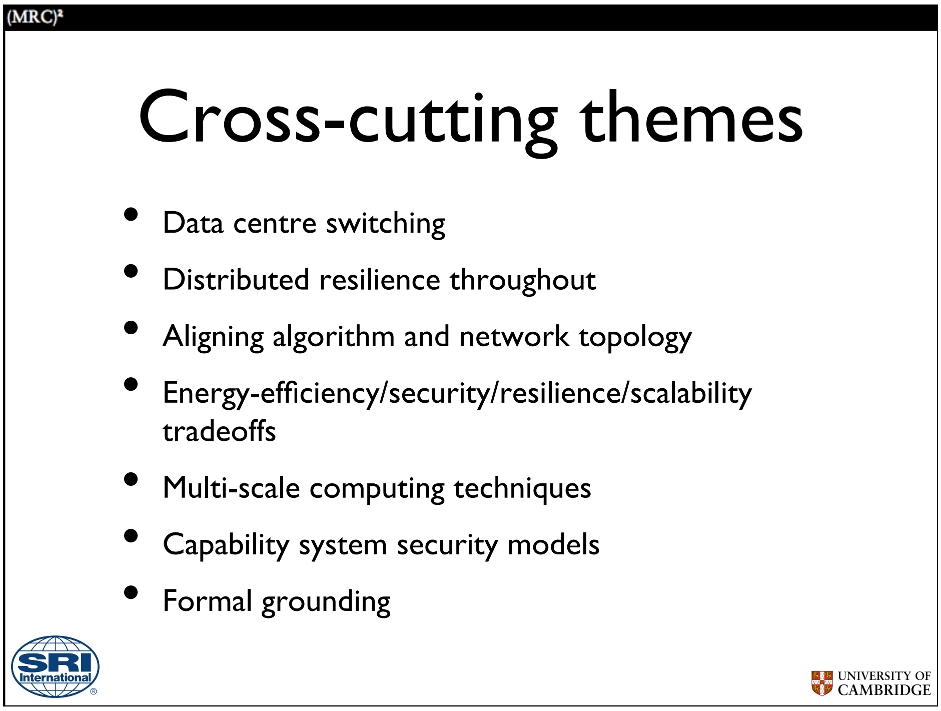
New framework programming secure clouds

New high-dimensional data centre switch fabric

New capability-oriented CPU memory interconnect

New trustworthy switches and switch controllers

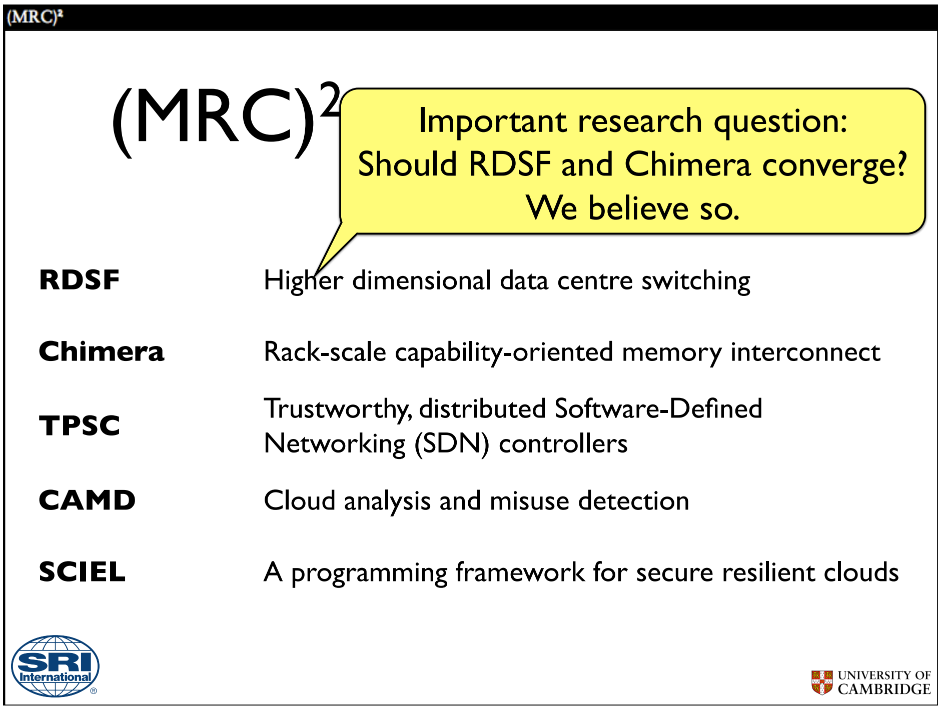
New distributed analysis, analytics, and misuse detection and response



(MRC)^2

Cross-cutting themes

- Data centre switching
- Distributed resilience throughout
- Aligning algorithm and network topology
- Energy-efficiency/security/resilience/scalability tradeoffs
- Multi-scale computing techniques
- Capability system security models
- Formal grounding



(MRC)^2

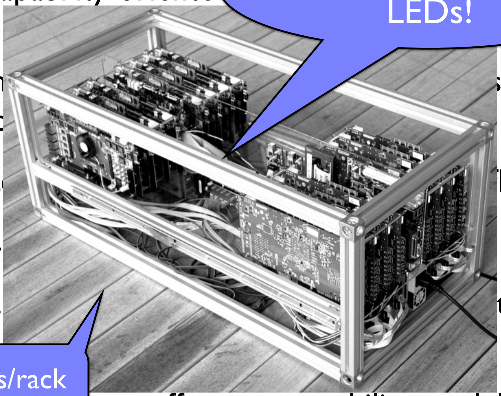
(MRC)^2

Important research question:
Should RDSF and Chimera converge?
We believe so.

RDSF	Higher dimensional data centre switching
Chimera	Rack-scale capability-oriented memory interconnect
TPSC	Trustworthy, distributed Software-Defined Networking (SDN) controllers
CAMD	Cloud analysis and misuse detection
SCIEL	A programming framework for secure resilient clouds

Chimera

Rack-scale capability-oriente



Has lots of blue LEDs!

- Start with … scale to multi-c
- Investigat … low
  - More s
  - Exploit … to CPU
  - …ency effects on capability model

16 FPGA/unit, 4 units/rack

Anticipated 128-256 cores, 16-32 threads/core

RDSF

Resilient distributed switching fabric

- RDSF is a **high-dimensional structure** with a switchlet for every compute node
  - Multi-path redundant topology for performance, resilience and security
  - Components are functionally interchangeable
  - High(er) performance through closer processor-network affinity
  - Remap network topology to match program data flow

Non-traditional world view!

(MRC)²

TPSC

Trustworthy programmable switch controllers

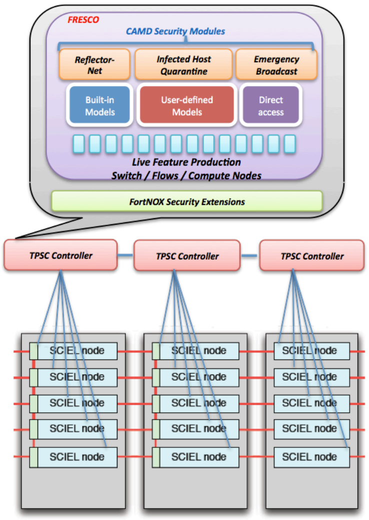
- Trustworthy platform for switch control
  - Platform for switch control applications
  - CHERI-based security model
- Distributed switch controllers
  - Integrated with RDSF: one-to-one with switchlets
  - Distributed control for resilience and performance
  - Scaling from one controller to one million?
- Formal grounding for both isolation and distribution properties

UNIVERSITY OF CAMBRIDGE

(MRC)²

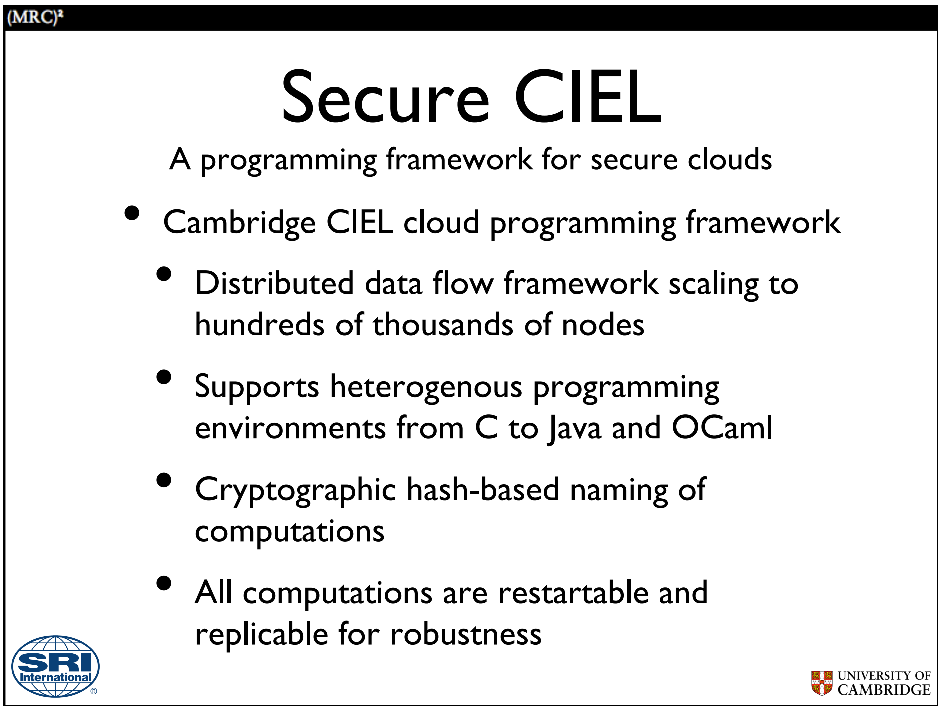
CAMD

Cloud analysis and misuse detection



- Existing approaches rely on centralised visibility and control
  - e.g., OpenFlow switches/ controllers
- Distribute both switch management functionality and analytics/misuse detection/ remediation
- CAMD offered by and for multiple tenants, as well as data center owners
  - e.g., APIs for IDSs, reflector nets, emergency broadcasts, IPSs, BotHunter, ...

UNIVERSITY OF CAMBRIDGE

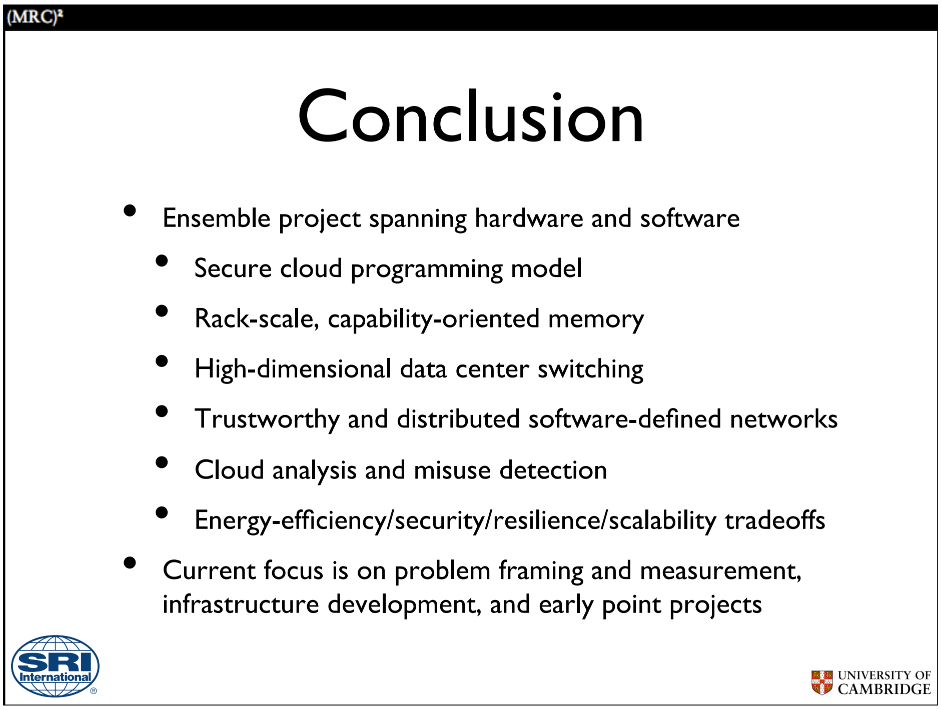


$(MRC)^2$

Secure CIEL

A programming framework for secure clouds

- Cambridge CIEL cloud programming framework
  - Distributed data flow framework scaling to hundreds of thousands of nodes
  - Supports heterogenous programming environments from C to Java and OCaml
  - Cryptographic hash-based naming of computations
  - All computations are restartable and replicable for robustness



$(MRC)^2$

Conclusion

- Ensemble project spanning hardware and software
  - Secure cloud programming model
  - Rack-scale, capability-oriented memory
  - High-dimensional data center switching
  - Trustworthy and distributed software-defined networks
  - Cloud analysis and misuse detection
  - Energy-efficiency/security/resilience/scalability tradeoffs
- Current focus is on problem framing and measurement, infrastructure development, and early point projects