An introduction to

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

Ross Anderson

Professor of Security Engineering

An introduction to

UNIVERSITY OF
CAMBRIDGE

Computer Laboratory

An academic Department within the University
that encompasses Computer Science,
along with related aspects of
Mathematics, Engineering, and Technology.

Menu

- Some history
- Teaching
- Research
- Entrepreneurship
- 2009 Research Students Fund

Some history

Mathematical Laboratory (1937-69)

In the beginning:

one Director...

J.E. Lennard-Jones (Prof. Theoretical Chemistry)

...and one staff member, M.V. Wilkes (University Demonstrator).

Mathematical Laboratory (1937-69)

In the beginning:

Mechanical calculators

Electronic Delay Storage Automatic Calculator (EDSAC)

Maurice Wilkes, May 1949

Practical computer:

- 650 instructions/s
- 1k x 17 bits
- paper tape input
- teletype output
- 4m x 3m
- 3000 valves
- 12kW

Mathematical Laboratory (1937-69)

Post-war:

One computer
to rule them all...
EDSAC ('49–'58)
EDSAC II ('58–'65)
Titan ('64–'73)

First ever book on
computer programming:
Wilkes, Wheeler, and Gill
(Addison-Wesley, 1951)

Professors Wilkes, Wheeler, and Needham in 1992

Bosses and Buildings

1937 Lennard-Jones

1946 Maurice Wilkes

1970 Computer Laboratory, New Museums Site

1980 Roger Needham

1995 Robin Milner

1999 Ian Leslie

2001 Move to the William Gates Building

(Computer Lab and Computing Service get divorced.)

2004 Andy Hopper

William Gates Building

Computer Laboratory today

Part of the *School of Technology* and the *Faculty of Computer Science & Technology*.

Staff

- 35 teaching officers (and counting)
- 35 contract researchers
- 10 computer officers + 15 administrative assistants

Students

- 155 research students
- 15 Diploma + 25 MPhil post-grads
- 300 undergraduates

Teaching

Taught courses

1949 DIY with EDSAC

1953 Post-graduate Diploma course

1964 Extra-departmental teaching computing for Natural Scientists

1970 University Computing Service utility computing for staff and students

1971 One-year course

1978 Two-year course

1985 MPhil in Speech & Language

1988 Three-year course (CST Parts IA, IB & II)

Our course aims

- To give our students an understanding of fundamental principles that will outlast today's technology.
- To produce graduates who will lead progress, not merely cope with it.

A Fourth Year?

Motivation

- growth of subject in both breadth and depth
- overlap with Engineering and other disciplines
- alternative first-year options
- development of specialist Masters' courses
- professional accreditation

Proposal

- retain three-year broad course
- more practical work including professional opportunity and research opportunity
- one-year research MPhil in specialised topics

Research

CL Framework for Computing

Science:

Curiosity-driven discovery of the "science of the artificial"

Technology:

Invention and transformation to drive innovation

Quality:

Professional and ethical development of computing

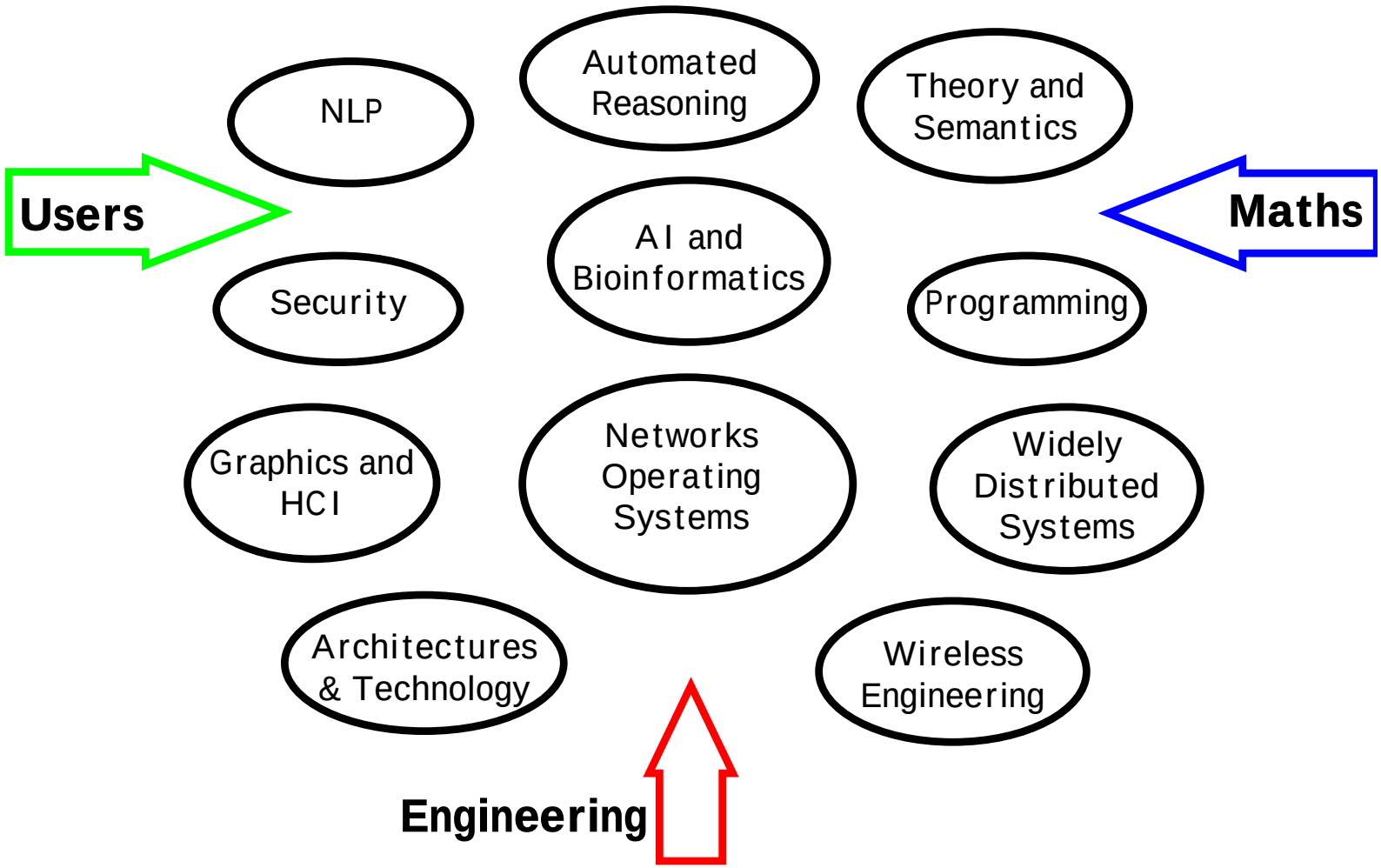
Dependability:

Efficient and dependable infrastructures

Sustainability:

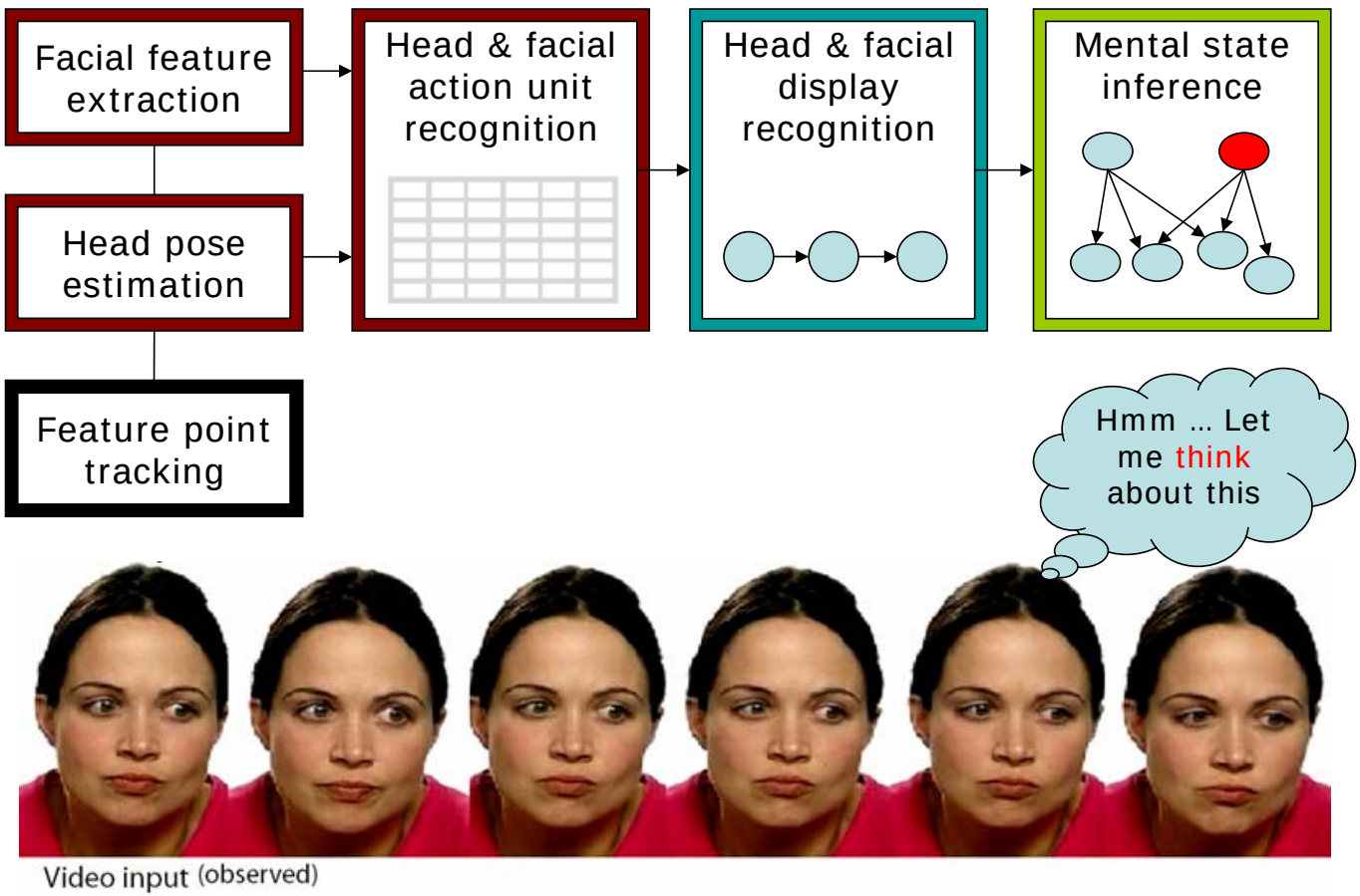
Support for development of physical world and society

CL Research themes



Mind-Reading Machines

R. el Kaliouby & P. Robinson



The Mindreading DVD

- Comprehensive labelled corpus
  - 412 mental states (or emotions)
  - 6 videos per mental state
  - 24 groups
    - meta-groups
    - fine shades of the same mental state
  - posed using 30 actors
  - classified by panel of 10

Mindreading DVD (Jessica Kingsley Publishers), courtesy of the Autism Research Centre, University of Cambridge www.human-emotions.com

RAINBOW

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Generalization

- CVPR 2004 corpus
  - 16 conference delegates (*not* actors)
  - each acting six mental state groups
- 96 videos tested on panel of 18 people
  - average accuracy 54%
  - 85% consensus only achieved on 11% of videos
- 88 videos tested on automatic system
  - 3 too short and FaceTracker failed on 5
  - average accuracy 64%
  - 80% accuracy for videos achieving consensus
- System as good as best 6% of panel

RAIN BOW

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

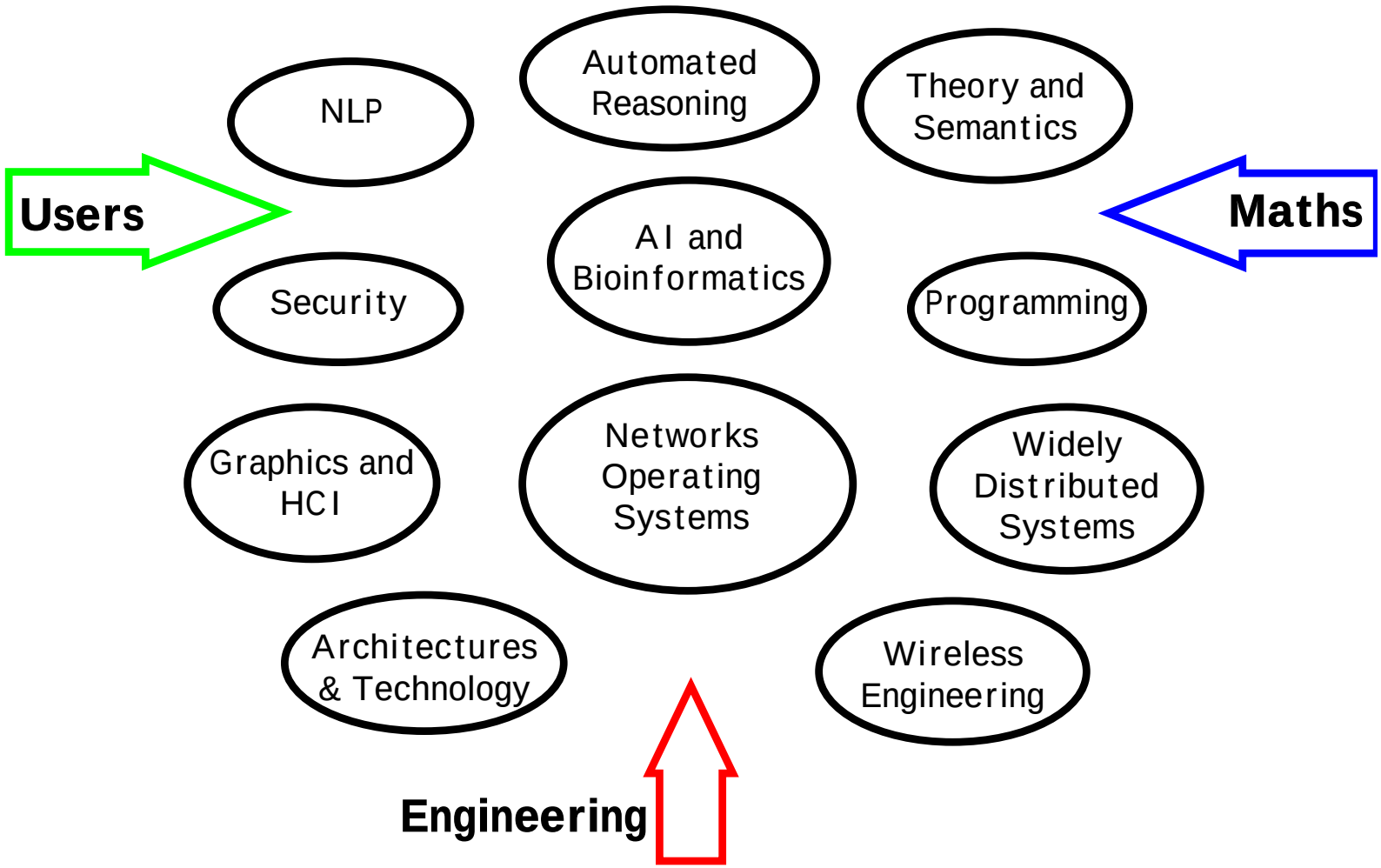
Driver monitoring

- Pleasure
  - enjoyable driving
- Comfort
  - easy driving
- Concentrating
  - neutral
- Bored
  - distracted thinking about something else
- Uncertain
  - distracted finding route
- Bothered
  - discomforted stuck in heavy traffic

RAIN BOW

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

CL Research themes



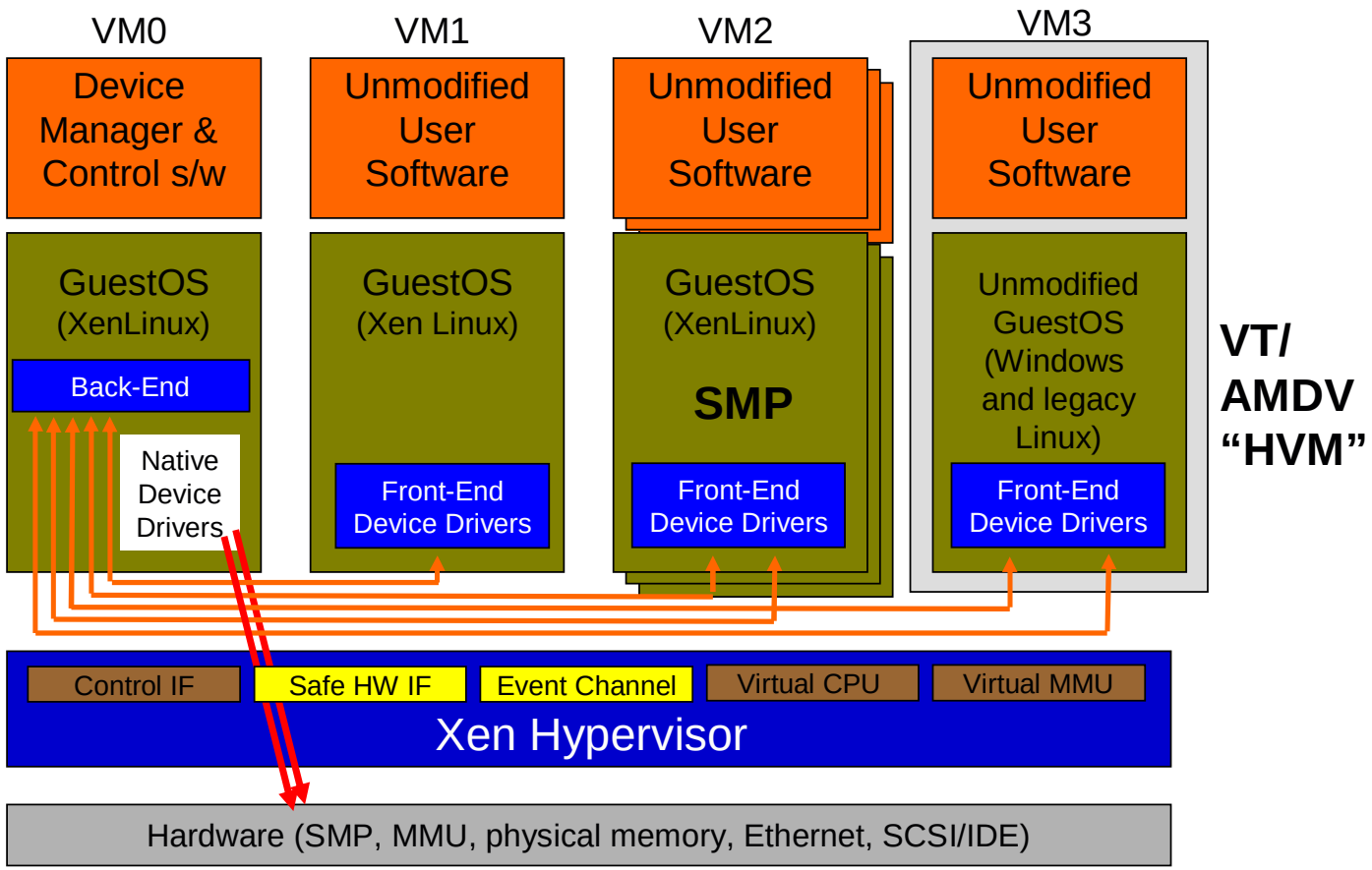
and the Art of Virtualization

Ian Pratt

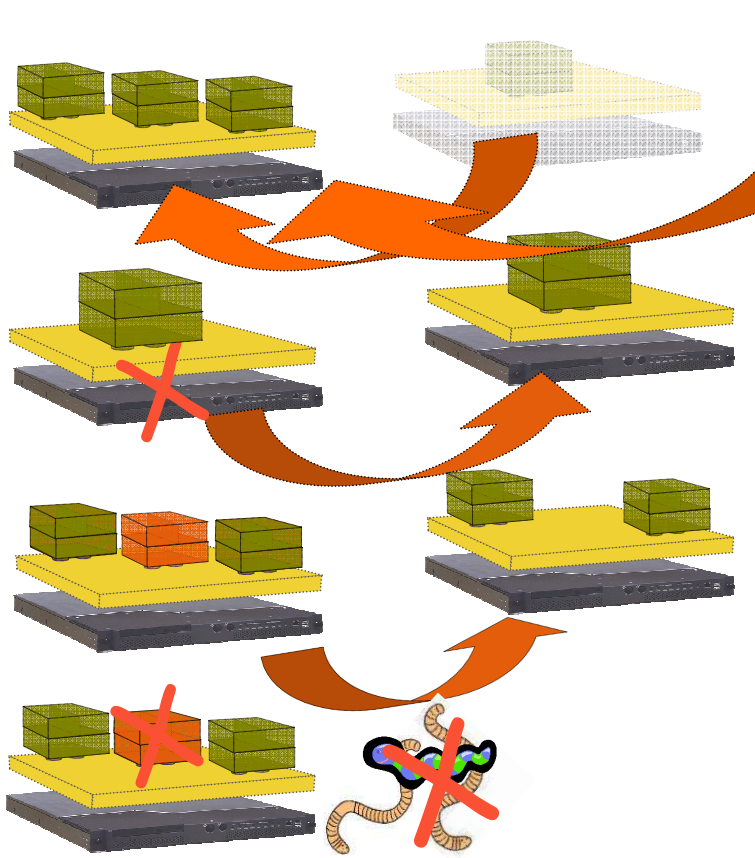
XenSource Inc and

University of Cambridge

Xen Architecture



Xen Use Cases

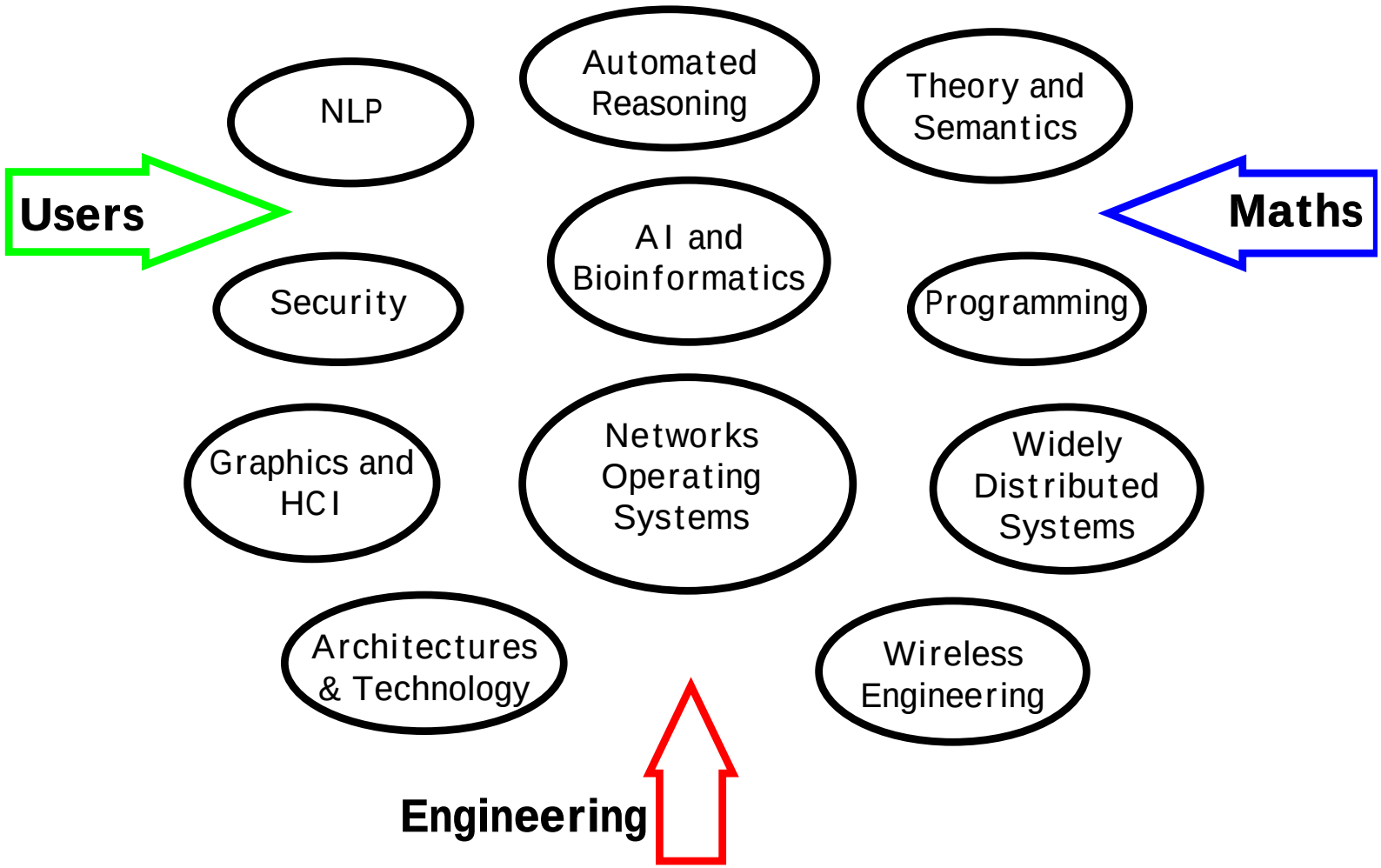


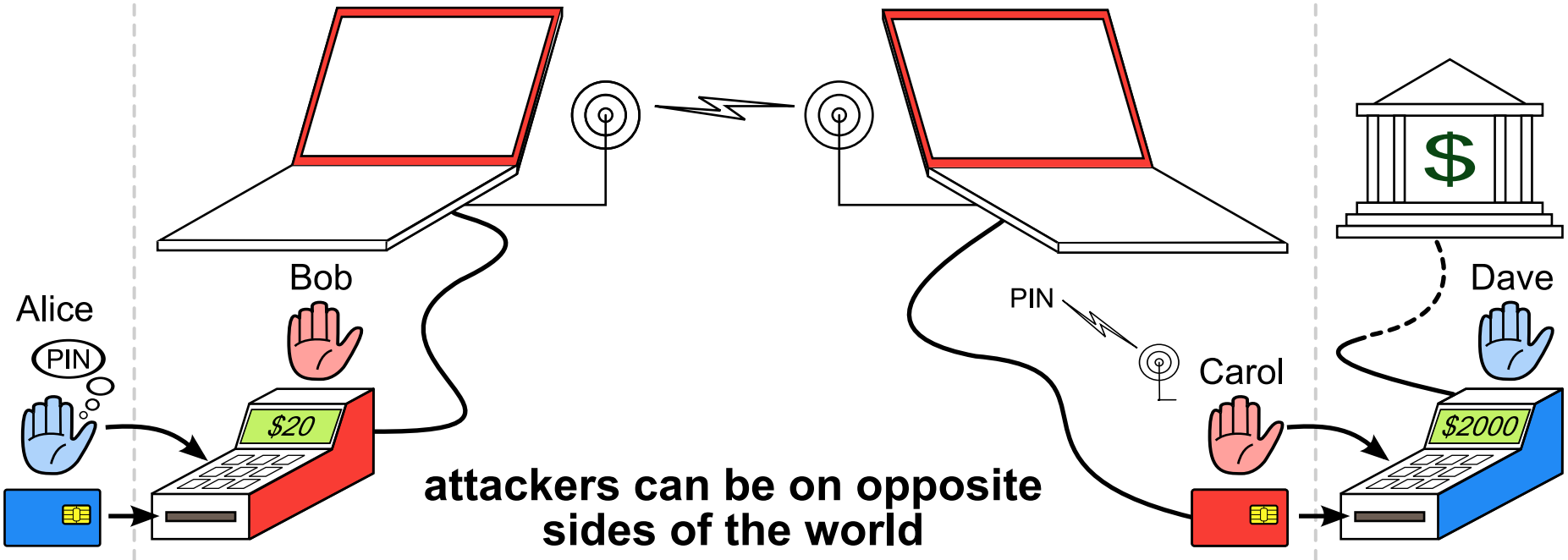
- Consolidate under-utilized servers
- Utilize multicore
- Avoid downtime with VM Relocation
- Dynamically re-balance *workload* to guarantee application SLAs
- Enforce security policy
- Debugging, monitoring

Xen Research Projects

- Whole-system pervasive debugging
  - Lightweight checkpointing and replay
  - Cluster/distributed system debugging
- Software implemented h/w fault tolerance
  - Exploit deterministic replay
  - Explore possibilities for replay on SMP systems
- Multi-level secure systems with Xen
  - XenSE/OpenTC : Cambridge, Intel, GCHQ, HP, …
- VM forking
  - Lightweight service replication, isolation
  - UCSD Potemkin honeyfarm project

CL Research themes




Alice
PIN
Bob
$20
PIN
Carol
Dave
$
$2000
attackers can be on opposite sides of the world

Security Economics

Many systems fail not for technical reasons so much as from misplaced incentives - often the people who could protect them are not the people who suffer the costs of failure. Many questions with an economic dimension as well as a technical one.

- Are open or closed systems more dependable?
- How often should we patch?
- How can we disrupt black markets?
- Why do people say they value privacy yet act otherwise?
- Why do 30% of large commercial system projects fail, but 70% of government projects?

Topology and Vulnerability

- Many real-world networks can be modeled as scale-free – social contacts, disease spread, spread of computer viruses
- Power-law distribution of vertex order, often arising from preferential attachment
- Highly-connected nodes greatly enhance connectivity
- … and also vulnerability – if you attack them, the network is rapidly disconnected

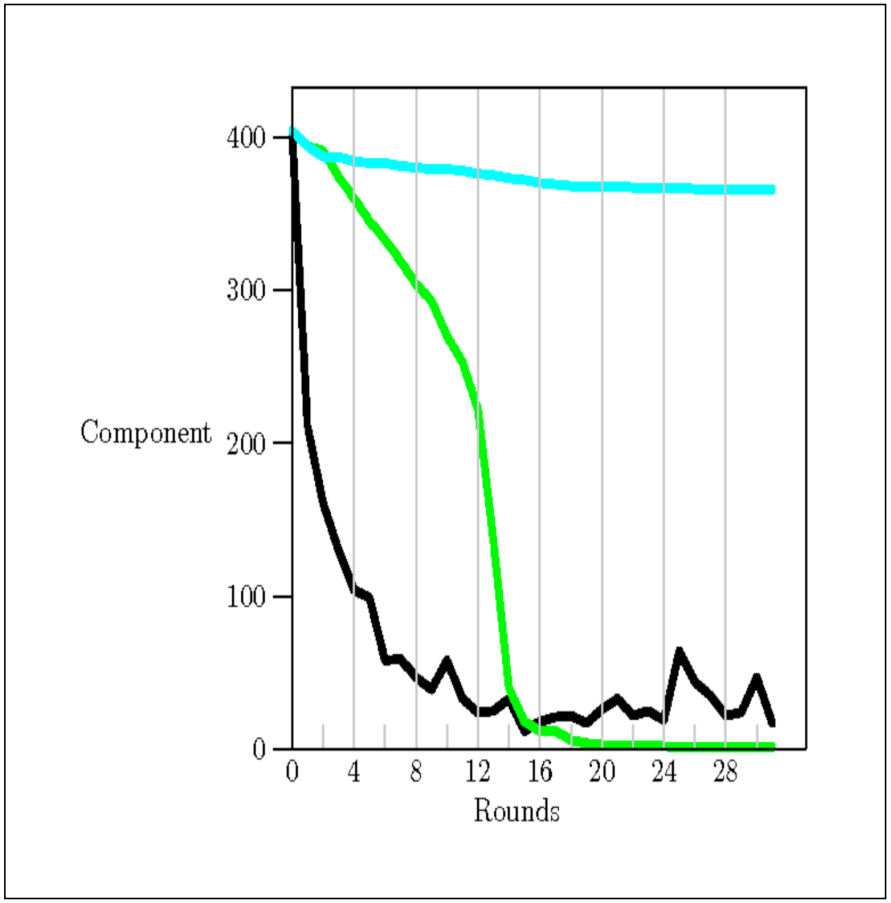
Topology and Vulnerability (2)

- Example: Sierra Leone HIV/AIDS program treated prostitutes first – only 2% of population infected (vs 40% in Botswana)
- Example: if you conquer a country, subvert or kill the bourgeoisie first
- What about the dynamic case, e.g. insurgency? Police keep arresting, insurgents keep recruiting
- This work: we apply evolutionary game theory to study this dynamic case

Simulation Methodology

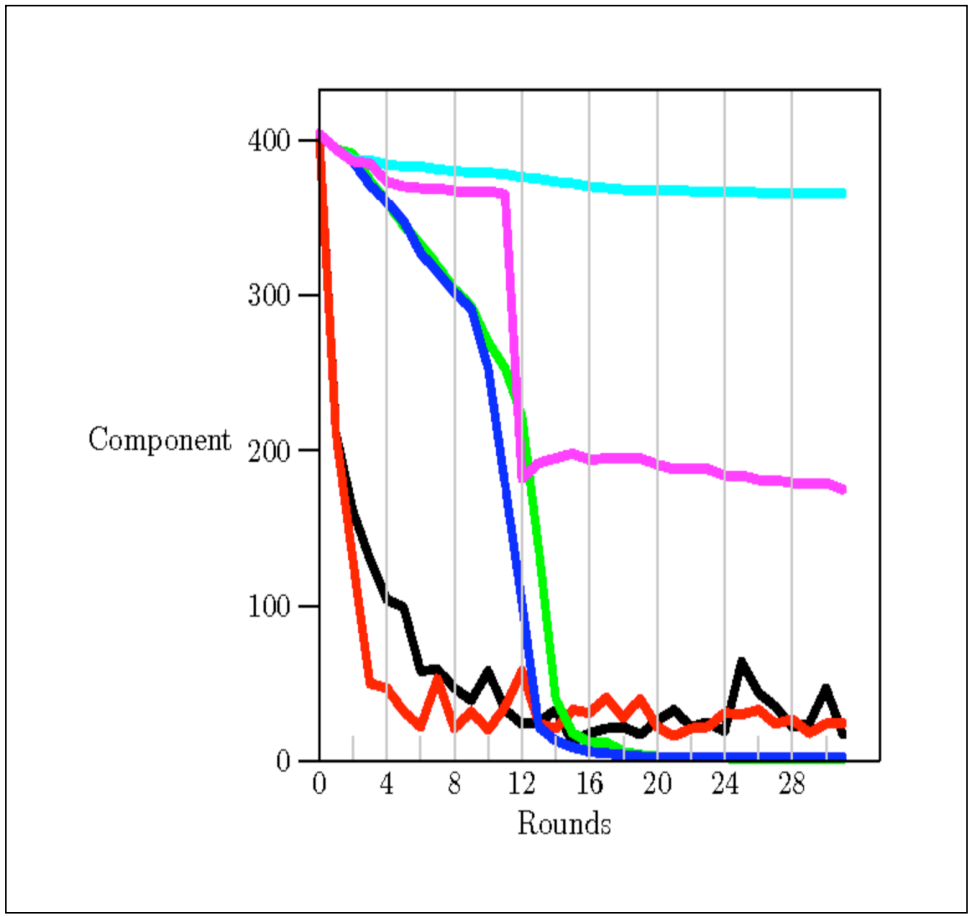
- After Axelrod's work on iterated prisoners' dilemma
- Scale-free network of 400 nodes
- At each round, attacker kills 10 nodes – their selection is his strategy
- Defender recruits 10 more, then reconfigures network – how he does this is his strategy
- Iterate search for defense, attack strategy

Evolving Defense Strategies



- Black – scalefree replenishment
- Green – replace high-order nodes with rings
- Cyan - replace high-order nodes with cliques
- Cliques work very well against the vertex-order attack

Evolving Attack Strategies



- Centrality attacks are the best counter we found to clique-based defenses
- Rings: G, B cliques: C, M
- Vertex-order attack: B, G, C
- Attack using centrality: R, B, M

Grand Challenges

- May take fifteen years or more to complete.
- Attract world-wide participation.
- Have a clear test of success or failure.
- Pursue scientific ideals.
- Enlarge fundamental understanding:
  - pursues scientific ideals
  - in an area of significance to mankind.

(Egs from other disciplines: prove Fermat's last theorem, map the human genome, find the Higgs boson.)

Entrepreneurship

Industry connections

- Computer Lab and alumni have created 130+ companies.

  For example, communications related ones:
  Bango.net, MobIsle Communications, Amrivox, Digital Mail, Applied Generics, Codian, Virata, Real VNC, IPV, Adaptive Broadband, Cambridge Broadband, Ubisense, Level 5 Networks, Sintefex, Audio, Nemesys, Patientline Plc, Cotares, Metrica Systems, Artimi, Equisys, FORE, UK Broadband Ltd, XenSource,. . .

- Computer Lab Industry Club
- Computer Lab Alumni Association (CL Ring)

2009 Research Students Fund

Computer Laboratory Appeal

University of Cambridge 800th Anniversary in 2009.

The 2009 Computer Laboratory Research Students Fund.

- Fund the elite PhD students.
- Our aim is £15M - we have raised £1.6M
- £500K endows one PhD studentship for ever.

Lunch