

Using Low-Cost Cryptographic Hardware to “Rob a Bank”

**Richard Clayton
& Michael Bond**



**UNIVERSITY OF
CAMBRIDGE**

Computer Laboratory

Presented at: MCS Oxford,
7th February 2002

Summary

- Keys and Ciphers
- The IBM 4758 Cryptoprocessor
- How PIN values work
- The low-cost hardware “DES cracker”
- How to extract 3DES keys from a IBM 4758
- Mike Bond’s “API attacks”

Keys and Ciphers

- Kerckhoff's doctrine (1883)
 - the security of a system should depend upon its key and not upon its design remaining obscure
- If there is no shortcut then the security of a system depends upon its key length
 - trying all possibilities @ 33 million keys/sec
 - $2^{40} = 9$ hours
 - $2^{56} = 69$ years
 - $2^{80} = 1.1$ billion years

A History of Tamper Resistance

Problem: another program on the same machine can access your sensitive data

- Put keys into separate microprocessor
- Put microprocessor into a tin box
- Photocells and tilt detection
- Epoxy “potting”
- Tamper detecting barriers

The IBM 4758

- Protective barrier with wires of chemically similar compound
 - Detectors for temperature & X-Rays
 - “Tempest” shielding for RF emission
 - Low pass filters on power supply rails
 - Multi-stage “ratchet” boot sequence
- = STATE OF THE ART PROTECTION!**



CCA and PIN values

- Common Cryptographic Architecture
 - runs on many IBM platforms
 - available for free to run on a 4758
- A PIN value (in the CCA world) is the account number encrypted with (112 bit) 3DES key and last few bytes made decimal
- Changing a PIN => changing an offset

Key Entry under CCA

- Each key is loaded in two parts, which are then XORed together
 - XOR means that knowing one part tells you NOTHING about the final key value
- Two security officers, “trusted” not to collude, are given one part of the key each.
 - They authenticate themselves and then separately load these into the 4758.
- This makes the key entirely secure...

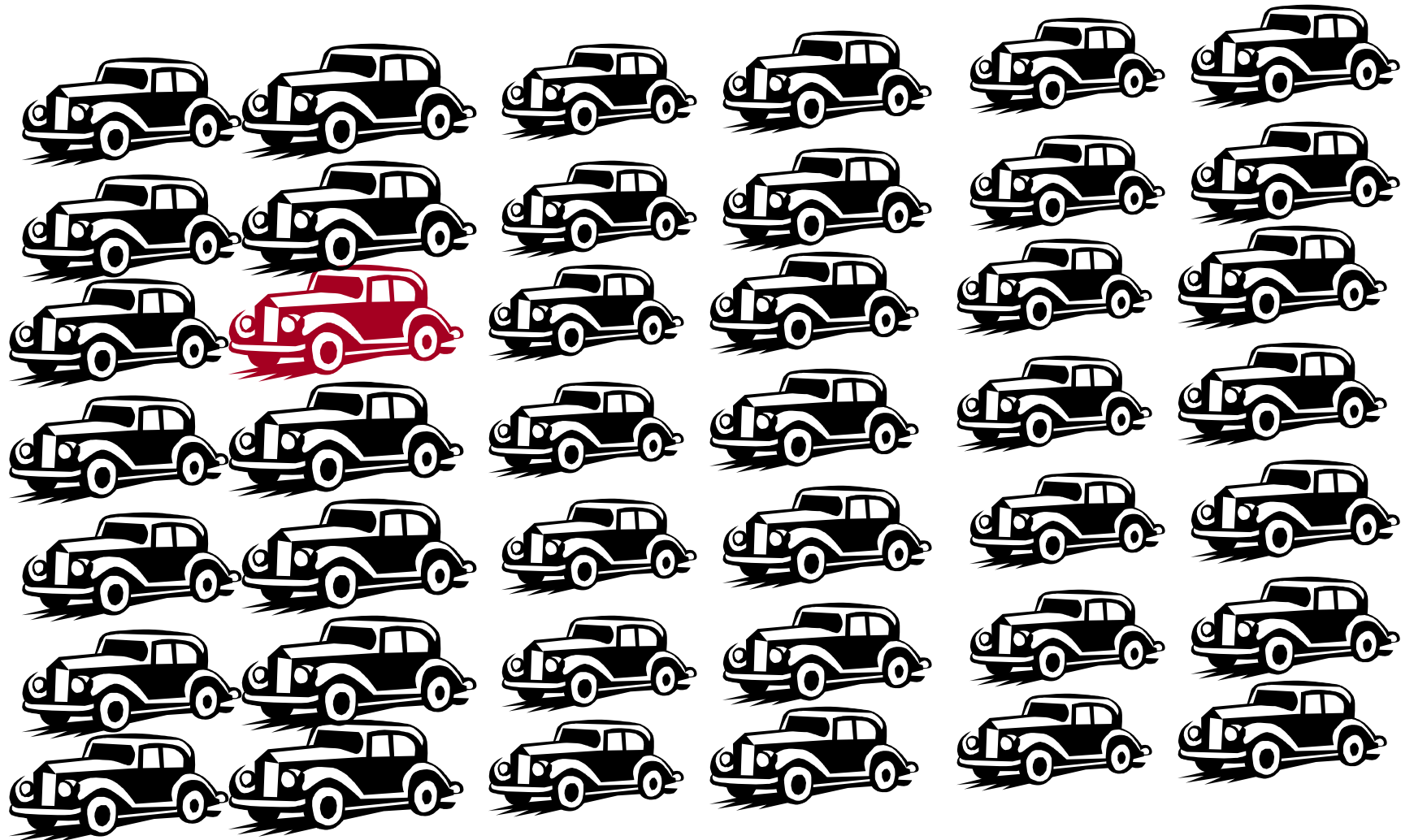
The Meet in the Middle Attack

- A thief walks into a car park and tries to steal a car...



- How many keys must he try?

The Meet in the Middle Attack



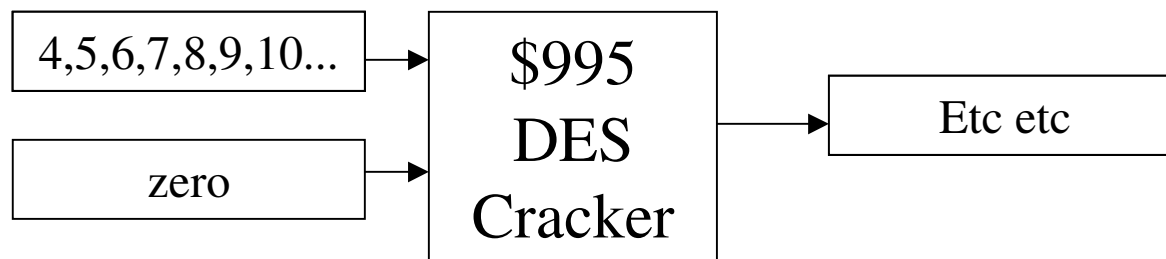
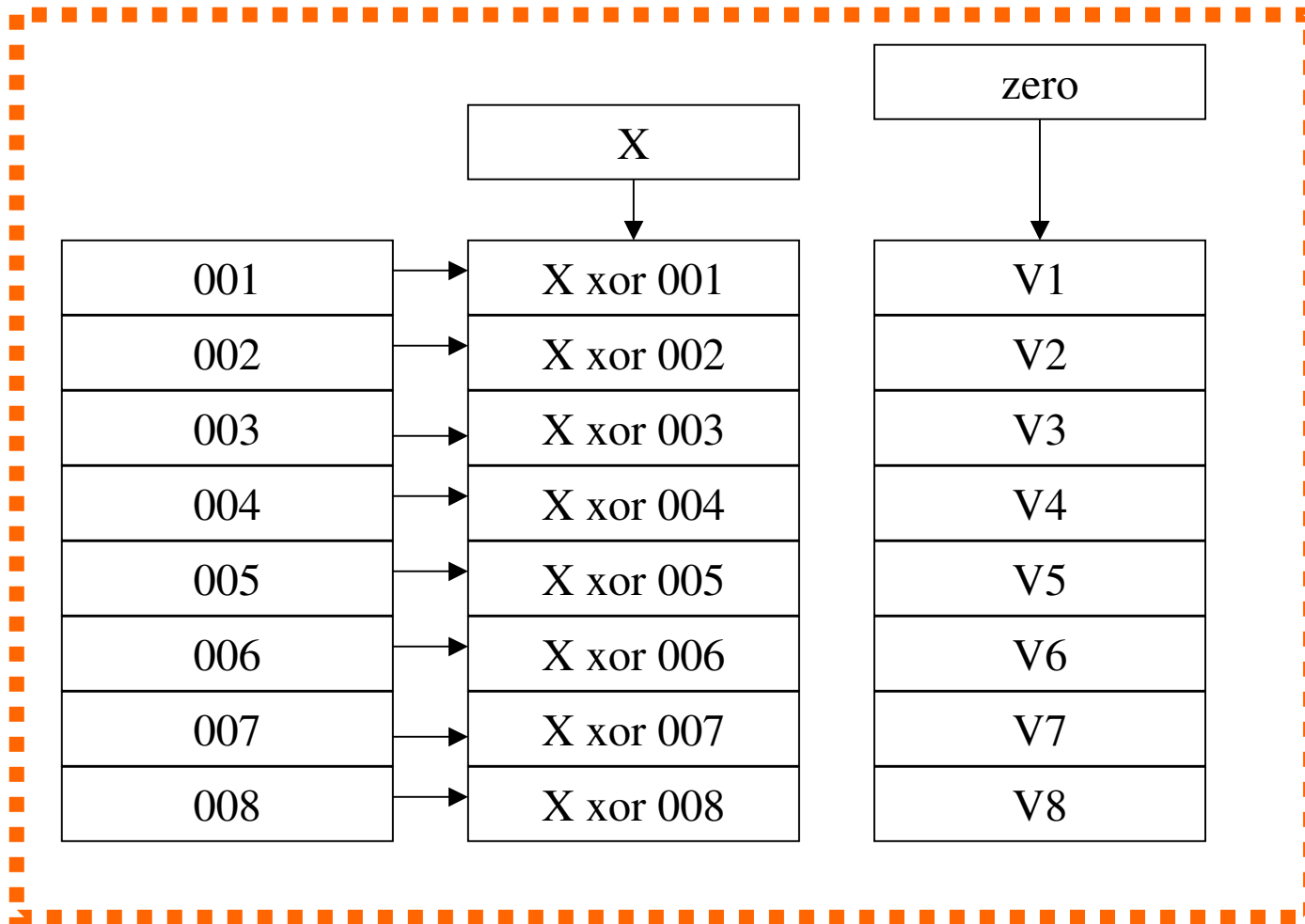
The Meet-in-the-Middle Attack

Idea: Attack multiple keys in parallel

- Encrypt the same plaintext under each of the multiple keys to get a “test vector”
- Attack by trying all keys in sequence but check for a match against any test vector value (check is faster than encrypt)
- Typical case: A 2^{56} search for one key becomes a 2^{42} search for 2^{14} keys

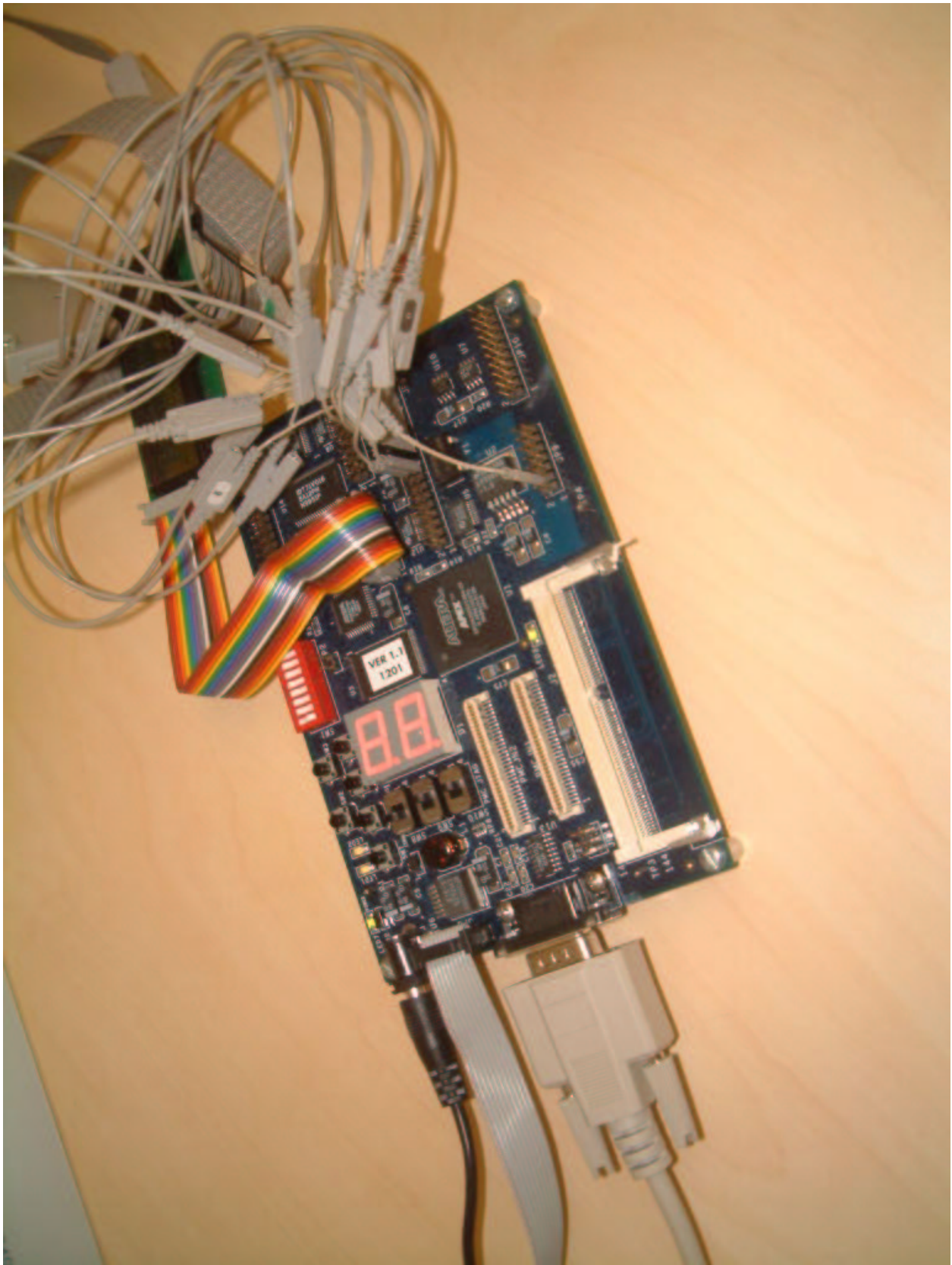
Attacking the CCA : Part 1

- Create unknown DES key part
- XOR in “...001”, “...002”, “...003” etc
- Encrypt zero value under each key
- Repeat to get 16384 (2^{14}) results
- Some complexity because of parity issues, but essentially simple & takes 10 minutes.
- Use “brute-force” attack to get the DES key



Low-cost DES Cracker

- \$995 Excalibur kit (Altera 20K200 FPGA)
 - chip cost is ~\$5 (in volume; \$178 one-off)
- 33MHz pipeline (& 60MHz possible)
- 2^{25} keys/second
 - 56 bit DES = 69 years
- However... look for 16384 keys in parallel
 - with average luck find first key in 25.4 hours



Attacking the CCA : Part 2

- Recall we had 16K related DES keys
- We can crack one of these in ~1 day
- Now create 16K related 3DES keys with “replicate” halves and “exporter” capability
 - 3DES = EncryptA; DecryptB; EncryptA
- Export the DES key under the 3DES keys
- Since replicate can also crack in ~1 day

Attacking the CCA : Part 3

- Create non-replicate 3DES key by combining two unequal halves with the replicate halves that we've now determined
- Export all the CCA keys under this key
- Download list of PIN offsets
- Use magnetic stripe writer to create cards
- Use any ATM to extract money from accounts
- Go to Bermuda!

Michael Bond's "API attacks"

- New type of attack: use standard API in non-standard way to cause dumb things
 - Overloaded key types
 - Unauthorised type casting
 - 3DES binding attack
 - Related keys

Mike's PhD topic targets formal methods that will detect (and avoid) these problems

Who am I?

- 2nd Year PhD student at the Computer Laboratory, University of Cambridge, Age:22
- Studied “Computer Science” as an undergraduate at Cambridge, before that KSB
- Studied Maths, Physics, Chemistry, DT, IT etc... at A-Level
- Currently live in Cambridge, a mile or so from town centre & computer lab

What is a PhD?

- In theory: “an original and significant contribution to the general body of knowledge in the chosen subject” – a thesis of 40,000-100,000 words
- In practice: three years of supervised research into a particular topic as a member of a research group studying similar topics.
- Year 1 – Explore
- Year 2 – Understand
- Year 3 – Write Up

My PhD

- “Understanding Security APIs”
- Security API = Software interface to a processor performing security functions, usually tamper-resistant hardware
- Year 1 : Analysed 6 different cryptoprocessors, published academic papers explaining attacks
- Year 2 : Producing design rules, and building analysis tools

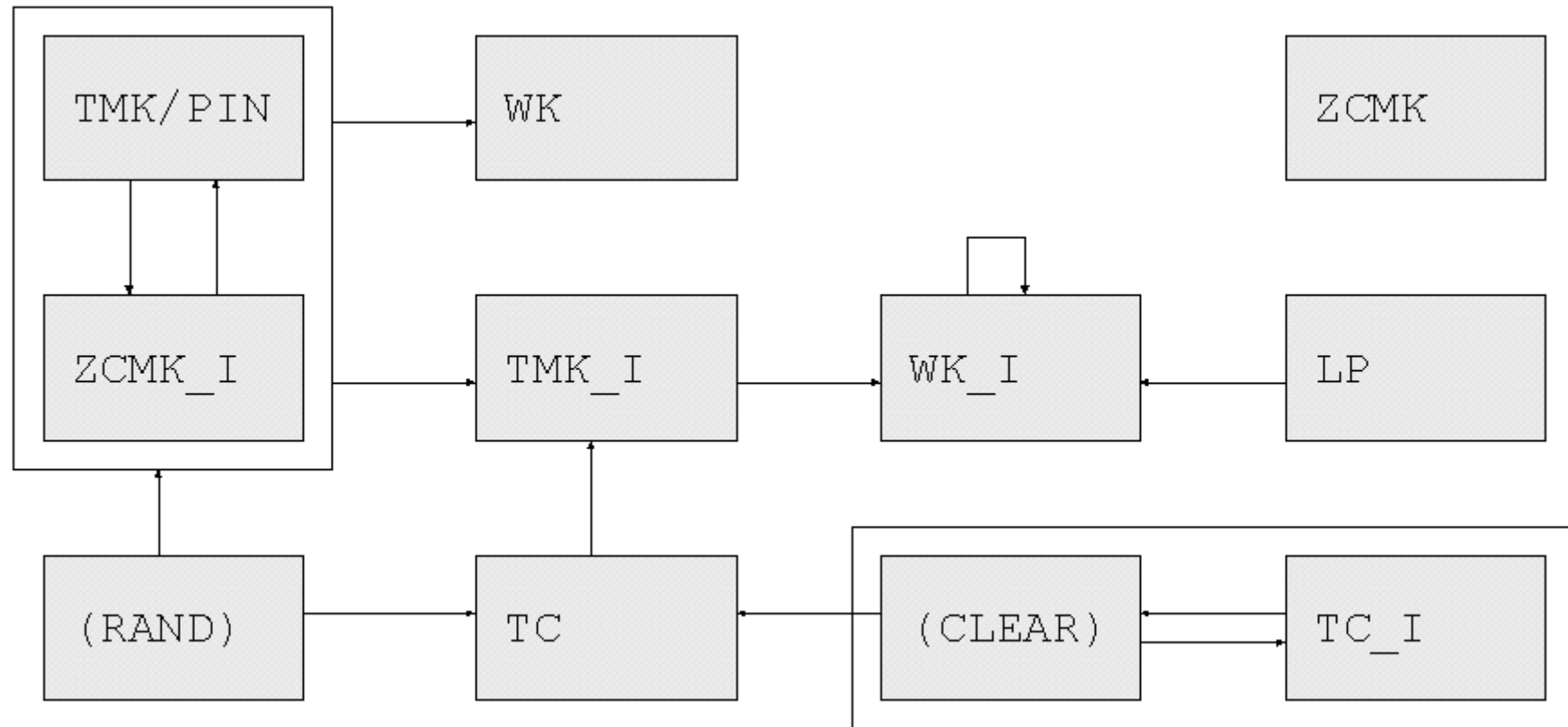
The PRISM Security Module



The Visa Security Module



VSM Type Diagram



Example Security API Commands

U→C : { A }_{KM} , { B }_{KM}

C→U : { A+B }_{KM}

U→C : GUESS , { ANS }_{KM}

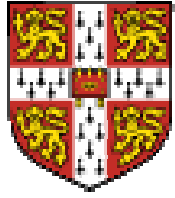
C→U : YES (if GUESS=ANS else NO)

U→C : { X }_{K1} , { K1 }_{KM} , { K2 }_{KM}

C→U : { X }_{K2}

Computer Security

- Cryptography, Anonymity, Protocols, Tamper-Resistance, Operating Systems, Copy-Protection
- Nowadays: Economics, Law, Politics
- Deals with fundamental conflicts of interest:
 - Good guys vs. bad guys
 - Competing corporations
 - International warfare
 - Personal privacy concerns



UNIVERSITY OF CAMBRIDGE

Computer Laboratory

- 30 academic staff = teaching/research
40 research assistants = research on lab money
80 research students = research on grant money
(+300 undergraduate students)
- Groups: Security, Graphics&Hardware,
Systems Research, Theory, Natural
Languages...



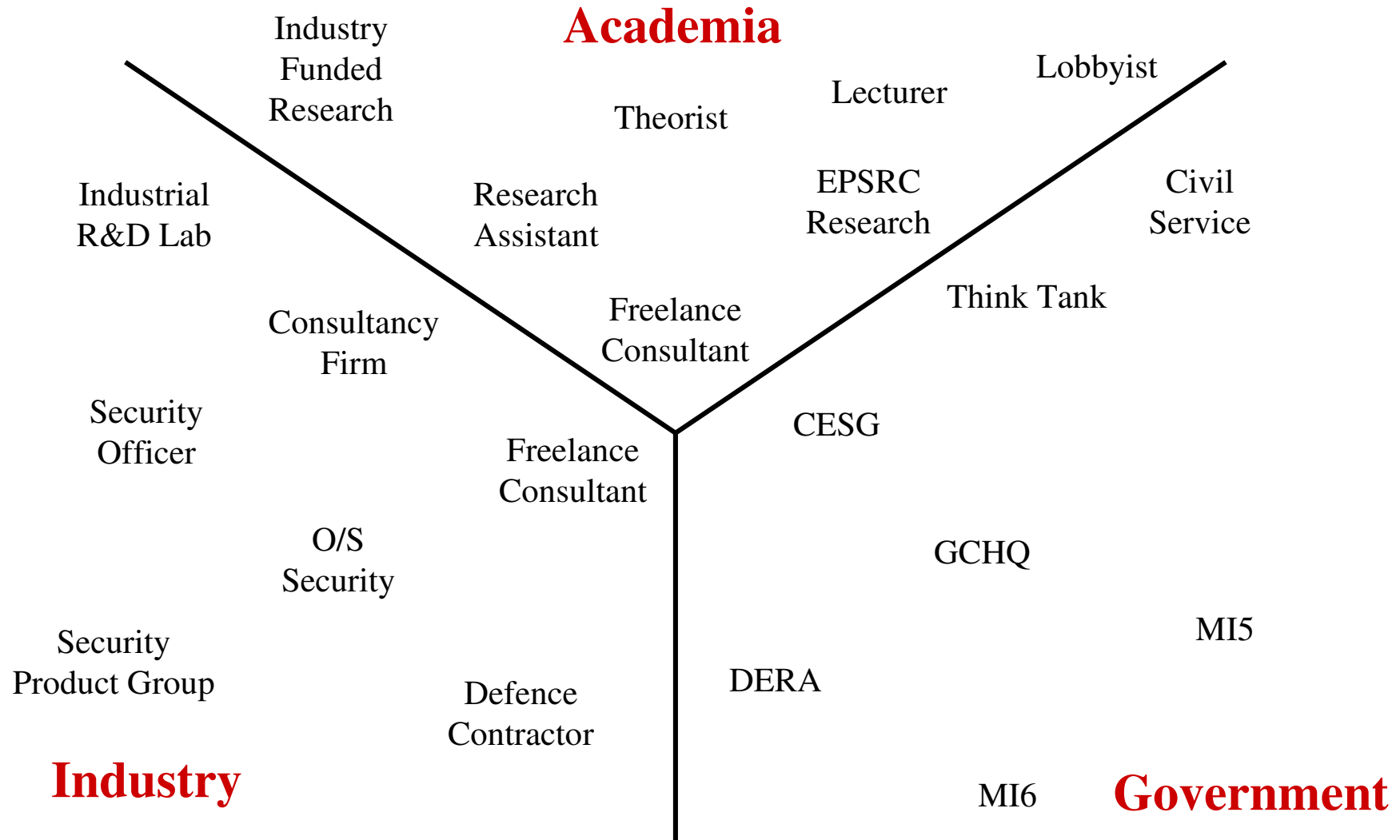
In My Office



What is Computer Science?

- Practical and theoretical study of the details and principles of software, hardware and communications technology
- Cambridge course aims to be technology independent, split 50/50 between practice and theory
- Includes a 60 man/h group project, and 500 man/h individual project

Computer Science Career Paths



Computer Hacking

- Not on the career path diagram?
- You can **really** hack hypothetical systems, and **really** hack real systems
- You need permission for the latter
- “Black Hats” and “White Hats” can both hack legally – difference is ethics of disclosure
- Real hackers are just common criminals

More Info

- How to hack a bank?

<http://www.cl.cam.ac.uk/~rnc1/descrack/>

- How to apply to Cambridge?

<http://www.cam.ac.uk/cambuniv/undergrad/>

- How to be like me?

<http://www.cl.cam.ac.uk/~mkb23/>

- More questions – email us:

Mike.Bond@cl.cam.ac.uk , Richard.Clayton@cl.cam.ac.uk