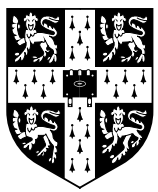
RIP Part III
“in an intelligible form”

Richard Clayton
Highwayman Associates Ltd



fipr thus™

Presented at: Government/Industry Forum, Gatwick, 10th Nov 2005

What's in this talk?

- Crypto history
- RIP history
- Safeguards
- Stored data *vs* "On The Wire"
- Some thoughts on Part III
- A way forward?

The Crypto Wars 1966-2000

- Spooks wanted crypto to stay in their sphere
  - Export controls: “crypto is a munition”
- US also attempted to gag academics
  - some success, but ultimately counterproductive
- US “Clipper” was an abject failure
  - failed to sell, and turned out to have flaws anyway
- US industry got export controls dropped
  - industry losing market share
  - Internet bubble demanded strong crypto

Meanwhile in the UK…

- Export controls in place for decades
  - COCOM, then Wassenaar (so you can't export BBC Micros to Yugoslavia or GameBoys to the Middle East, or PlayStations to Saddam)
- US exported their policy, forgot to tell us they'd changed their minds & we started to implement it five years later!
- So clearly we needed "key escrow"…

UK Crypto Policy

- Maundy Thursday 1997
  - "Licensing of Trusted Third Parties for the Provision of Encryption Services", all keys to be held by TTPs
- COJET (1999) told Blair to drop controls
- Draft Electronic Communications Bill 1999
  - Part I : TTPs (statutory voluntary licensing)
  - Part II: Electronic Signatures & Writing
  - Part III: Access to Keys
  - Part IV: Changes to the Telecommunications Act
    - the telco's didn't respond to consultations!

Solomon revisited: Two Bills

- DTI: Electronic Communications Act 2000
  - Part I: fall-back provisions for licensing, now defunct
  - Part II: Electronic signatures (yawn)
  - s14 categorically states “No Key Escrow”
- Home Office: RIP Act 2000
  - Part I: Interception + Communications Data
  - Part II: Surveillance (for HRA compliance)
  - Part III: Access to Keys
  - Part IV: Lots of Commissioners (etc)

Part III as finally passed

- Emphasis now clearly on decryption or "putting into an intelligible form"
- GAK (Government Access to Keys) needs a Chief Constable's signature & must be reported PDQ to Interception Commissioner
- Must serve GAK notices at board level
- "Tipping off" clauses can accompany GAK

Code of Practice

- All the hard questions punted to CoP
  - when will GAK be appropriate?
  - do you get to see the unintelligible form?
  - how will key entry for decryption be kept private?
  - what about multi-nationals?
  - what standard of care will keys receive?
  - and many, many more (see Hansard & UKCrypto)
- Home Office has poor record on RIP CoP
  - Part I Chapter I : 637 days, Chapter II: 676 & counting

A clash of cultures

- Spooks are used to symmetric crypto with hierarchical key distribution systems
- They expected to see companies managing keys for their clients (so escrow easy)
- But much crypto uses session keys and a PKI (ad hoc perhaps) to authenticate
  - when companies do have secrets, they protect them!
- Industry just didn't develop as expected

Part III isn't in force

and sky is still up there!

- Lobbying against RIP detailed the risks to industry (master keys stay in NYC or CH)
  - LSE/British Chambers of Commerce (£46 billion)
- Law Enforcement still short of scenarios
  - Turkish lorry driver, paedophile with encrypted disk
  - Cannot recall "The Sun" splashing on this topic…
- Credibility of offence is very limited
  - Won't people just take the 2 years ? (or now, 5)
  - Tories wanted to make it 10 for just that reason!

What law do we need ?

- Main requirement is to decrypt stored data
  - "on the wire" too complex (scenario-wise & technically)
- Perhaps just need an enabling notice?
  - to let the professionals off the hook
- GAK is a great deal of the problem
  - drop GAK and much of the economic risk evaporates
- Too few examples to frame a law yet
  - Main history lesson is that we are legislating too early!

Human Rights Act 1998

- Forcing to decrypt is supposed to be like forcing to provide DNA…
- Home Office lawyers (especially those of the 2000 era) not always mainstream
  - Will the House of Lords see it that way?
  - Will Strassbourg see it that way?
- Would a reworking of the Act's provisions make it more likely to escape challenge ?

What of Part III ?

- Half the world thinks Part III is already in force – that's damaging, we should scrap it
  - we're supposed to be best place to do eBusiness
- But "something must be done"
  - deploy lots more crypto; it's so hard for amateurs to use properly, that the intelligence take will go up!
  - spend the money on a Government run VoIP rendezvous site (it's the traffic data stupid!)

More at…

http://www.cl.cam.ac.uk/~rnc1/