Some open problems with RIPA Pt.3

Caspar Bowden

(Director FIPR 1998-2002)

Scrambling for Safety - 14th August 2006

(this presentation reflects personal views only)

- Some history
- Possession At Notice’s Time of Serving
- Protected information
- VAMP attacks and defences
- Public policy on Identity Management
- Fairness and arbitrariness

Some history

- Idea of coercing key disclosure had muddled evolution through two draft DTI E-Commerce bills 1998-1999, before Home Office took over 1999
- Power to reverse burden of proof first mooted in Cabinet Office PIU report 1999, following collapse of key-escrow policy (1995-1999)
- Over 1000 news articles concerning RIPA over 18 months
- Vigorous and unusually well-informed debate on RIPA in House of Lords in 2000
- Crucial amendment curbing RIPA Pt.3 lost in HoL by one vote
- Lots of material at www.fipr.org/rip/
  - But many dead links ☹

Possession At Notice's Time of Serving (PANTS)

- Burden-of-proof controversy – who said what (http://www.fipr.org/rip/burdenproof.html)
  - Charles Clarke maintained never an issue – only a matter of "parliamentary arithmetic" (http://www.fipr.org/rip/#ClarkingDevice) and that "propaganda is needed"
  - He thought that a password is present in-clear in a computer system – didn't understand basics of cryptography
- What will suffice to "adduce sufficient evidence to raise the issue" of non-possession?
  - Bad memory and or old data – please have mercy?
  - Key backup seems to have failed?
  - "the key just doesn't seem to work"?
- Will the jury take judge's direction?
  - "obviously defendant has something to hide"
- Will prejudicial information about past behaviour be admissible?

What is “protected information” ?

- Another burden-of-proof ambiguity? Circular definition?
  - *“key", in relation to any electronic data, means any key, code, password, algorithm or other data the use of which (with or without other keys)- (a) allows access to the electronic data, or (b) facilitates the putting of the data into an intelligible form;*
  - *"protected information" means any electronic data which, without the key to the data- (a) cannot, or cannot readily, be accessed, or (b) cannot, or cannot readily, be put into an intelligible form;*
  - RIPA S.49 “*This section applies where any protected information….*
    - *If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds- (a) that a key to the protected information is in the possession of any person..”*
- Distinguishing encrypted data and random numbers
  - 1-time pad
    - has it been used already or is it for future use?
  - “information hiding” - steganography
    - Is information hidden in MP3s/videos etc?
  - Encrypted filing systems with “too much space”
    - Is the “hidden compartment” full of data or random padding?
  - Arguments about stego-detection stats, and bandwidth for hiding

Anatomy of VAMP-ware

(Virus Ate My Password)

- Moriarty wants to frame Alice
  - Infect A’s machine with memory-resident code
  - Malware
    - Waits until A using machine
    - uses buffer-stuffing or standard API to change key/password
    - Phones home to M when successful
    - Deletes itself from memory
  - Moriarty arranges tip-off to law-enforcement
  - A arrested, machine seized, key demanded
  - No forensic traces of malware on A’s machine
    - Traces that key was changed – but A was using at the time
  - S.49 notice is served
  - Plead VAMP at trial
  - What “evidence” can Alice adduce?
- M can use to blackmail A?

VAMP-ware variations

- Terence wants “reasonable doubt deniability” against a S.49 Notice
- T infects own machine with VAMP-ware which *does* leave forensics
  - key-logger captures password each app use
  - silently “changes” password to same thing each time
  - sends secret phone-home messages to imagined Moriarty
  - forensics will show password did change each app use
- T arrested, gives wrong password (doesn’t work)
- At S.53 trial, after forensics discover VAMPware, T’s expert witnesses adduce that machine was infected
  - doesn’t matter that leave traces of repeated changes, since defence is T was unaware of silent infection
- Implausible but reasonable doubt that VAMPware struck last time before arrest, especially if malice suggested
  - police may be unwilling/unable to prove true source of intelligence about T (e.g. compromises CHIS)

Public policy and Identity Management

  - RIPA pt.3 applies to any password/key to authenticate access to information online
  - Information may be offshore, easier to serve suspect with S.49 for key than serve decrypt notice offshore
- Today:
  - encryption little used + weak passwords
- successful VAMP defence would nullify S.49?
  - high-profile miscarriage-of-justice case?
- Future:
  - users have many credentials, context specific, interfaces designed for routine use
  - will RIPA deter mass of honest users from properly securing information
  - In UK, will you need your ID Card to log into anything online?
    - each time pings the NIR "audit trail"
    - Observer story on Gordon Brown's plans for expansion

Authentication Threat List 1.0 – Christopher Drake (2/7/06)

1. Confidence Tricks

1.1. phishing emails
1.1.1. to lure victims to spoof sites
1.1.2. to lure victims into installing malicious code
1.1.3. to lure victims towards O/S vulnerabilities to inject malicious code
1.1.4. to lure victims into revealing information directly via reply or via embedded FORMS within the email

1.2. telephone phishing
1.2.1. to directly extract auth info
1.2.2. to direct victim to spoof site

1.3. person-to-person phishing / situation engineering
1.3.1. to directly extract auth info (ask)
1.3.2. to direct victim to spoof site
1.3.3. shoulder surfing (aka 4.5.2)
1.3.4. physical attack - see 4.7

1.4. typographic attacks
1.4.1. spoofing (eg: paypa1.com - using a number 1 for a little L)
1.4.2. direct download of malicious code
1.4.3. browser exploit injection

1.5. online phishing
1.5.1. pop-up/pop-behind windows to spoof sites
1.5.2. floating <DIV> or similar elements (eg: emulating an entire browser UI)

2. Remote Technical Tricks….

1. Confidence Tricks

1.1. phishing emails
1.1.1. to lure victims to spoof sites
1.1.2. to lure victims into installing malicious code
1.1.3. to lure victims towards O/S vulnerabilities to inject malicious code
1.1.4. to lure victims into revealing information directly via reply or via embedded FORMS within the email

1.2. telephone phishing
1.2.1. to directly extract auth info
1.2.2. to direct victim to spoof site

1.3. person-to-person phishing / situation engineering
1.3.1. to directly extract auth info (ask)
1.3.2. to direct victim to spoof site
1.3.3. shoulder surfing (aka 4.5.2)
1.3.4. physical attack - see 4.7

1.4. typographic attacks
1.4.1. spoofing (eg: paypa1.com - using a number 1 for a little L)
1.4.2. direct download of malicious code
1.4.3. browser exploit injection

1.5. online phishing
1.5.1. pop-up/pop-behind windows to spoof sites
1.5.2. floating <DIV> or similar elements (eg: emulating an entire browser UI)

2. Remote Technical Tricks

2.1. spoof techniques
2.1.1. vanilla fake look-alike spoof web sites
2.1.2. CGI proxied look-alike web site (server CGI talks to real site in real time - "man in the middle attack")
2.1.3. popup windows hiding the address bar (3.4.1/3.4.2)
2.1.4. <DIV> simulated browsers (1.5.2)

2.2. iframe exploits (eg: 1.5.1/1.1.3) (spammers buy iframes to launch 1.5 and 1.4 attacks)
2.3. p2p filesharing publication of products modified to remove/limit protection - PGP, IE7, Mozilla, ...
2.4. DNS poisoning (causes correct URL to go to spoof server)
2.5. traffic sniffing (eg: at ISP, telco, WiFi, LAN, phone tap...)
2.6. proxy poisoning (correct URL returns incorrect HTML)
2.7. browser exploits (correct URL returns incorrect HTML)
2.8. targeted proxy attack
2.8.1. directs to vanilla spoof web site (2.1.1)
2.8.2. uses CGI re-writing to proxy legitimate site (eg: convert HTTPS into HTTP to activate traffic sniffing) (2.1.2)
2.8.3 activates 5.7
2.9. Authorized exploitation - see 3.5.

3. Local Technical Tricks

3.2. Software vulnerabilities (aka exploits - eg - 1.1.3)
3.1.1. Known
3.1.2. Unknown

3.2. Browser "toolbars" (grant unrestricted DOM access to SSL data)

3.3. Trojans
3.3.1. Standalone modified/hacked legitimate products (eg: PGP or a MSIE7) with inbuilt protection removed/modified.
3.3.2. Bogus products (eg: the anti-spyware tools manufactured by the Russian spam gangs)
3.3.3. Legitimate products with deliberate secret functionality (eg: warez keygens, sony/CD-Rom music piracy-block addins)
3.3.4. Backdoors (activate remote control and 3.4.1/3.4.2)

3.4. Viruses
3.4.1. General - keyloggers, mouse/screen snapshotters
3.4.2. Targeted - specifically designed for certain victim sites (eg paypal/net banking) or certain victim actions (eg: password entry, detecting typed credit card numbers)

3.5. Authorized exploitation (authority (eg: Microsoft WPA/GA, Police, ISP, MSS, FBI, CIA, MI5, Feds...) engineer a Trojan or Viral exploit to be shipped down the wire to local PC, potentially being legitimately signed/authenticated software.)

3.6. Visual tricks
3.6.1. browser address bar spoofing
3.6.2. address bar hiding

3.7. Hardware attacks
3.7.1. keylogger devices
3.7.2. TEMPEST
3.7.3. malicious hardware modification (token mods, token substitution, auth device substitution/emulation/etc)

3.8. Carnivore, DCS1000, Altivore, NetMap, Echelon, Magic Lantern, RIPA, SORM...

4. Victim Mistakes

4.1. writing down passwords
4.2. telling people passwords
4.2.1. deliberately (eg: friends/family)
4.2.2. under duress (see 4.7)
4.3. picking weak passwords
4.4. using same passwords in more than one place
4.5. inattentiveness when entering passwords
4.5.1. not checking "https" and padlock and URL
4.5.2. not preventing shoulder surfing
4.6. permitting accounts to be "borrowed"
4.7. physical attack (getting mugged)
4.7.1. to steal auth info
4.7.2. to acquire active session
4.7.3. to force victim to take action (eg: xfer money)
4.8. allowing weak lost-password "questions"/procedures

5. Implementation Oversights

5.1. back button
5.2. lost password procedures
5.3. confidence tricks against site (as opposed to user)
5.4. insecure cookies (non-SSL session usage)
5.5. identity theft? site trusts user’s lies about identity
5.6. trusting form data
5.7. accepting auth info over NON-SSL (eg: forgetting to check $ENV{HTTPS} is ’on’ when performing CGI password checks)
5.8. allowing weak lost-password "questions"/procedures
5.9. replay
5.10. robot exclusion (eg: block mass password guessing)
5.11. geographical exclusion (eg: block logins from Korea)
6.12. user re-identification - eg - "We’ve never seen you using Mozilla before"
6.13. site-to-user authentication
6.14. allowing users to "remember" auth info in browser (permits local attacks by unauthorised users)
6.15. blocking users from being allowed to "remember" auth info in browser (facilitates spoofing / keyloggers)
6.16. using cookies (may permit local attacks by unauthorised users)
6.17. not using cookies (blocks site from identifying malicious activity or closing co-compromised accounts)

6. Denial of Service attacks

6.1. deliberate failed logins to lock victim out of account
6.2. deliberate failed logins to acquire out-of-channel subsequent access (eg: password resets)

Arbitrary punishment is unfair

- Terrorism Act 2006 increased S.49 penalty to 5 years
  - S.15(2): *"grounds ..were or included a* ***belief*** *that the imposition of the requirement was necessary in the* ***interests*** *of national security"*
- Given exactly the same evidence about whether a person is deliberately breaching a S.49 Notice…
  - how can it be fair to imprison for 5-years rather than 2-years?
- If they *were* guilty of "national security" offence…
  - but begging the question of proof-of-guilt of "underlying" offence
  - conviction will be for failure to comply with S.49
- Penalty will be **arbitrary**, on the same facts, depending on what person is charged with
  - designed for intimidatory effect
  - accused can only exonerate if they do have the key

Arbitrary punishment is unfair (2)

Current consultation (para.17) proposes that if :

- *(i) that person has been previously convicted of an offence contrary to section 1 of the Protection of Children Act 1978 or section 160 of the Criminal Justice Act 1978, or*
- *(ii) the apparatus or device containing the protected information contains an indecent photograph or pseudo-photograph of a child, or*
- *(iii) the apparatus or device containing the protected information has come into possession of any person together with other apparatus or a device which contains an indecent photograph or pseudo-photograph of a child, or*

- **Why are these criteria relevant for aggravating guilt for withholding a key (s.53)?**
  - *(iv) the court is satisfied that the* ***protected information is likely to contain*** *an indecent photograph or pseudo-photograph of a child (on the basis, for example, of evidence from a witness);*
- (iv) is relevant, but burden-of-proof issue again: balance-of-probabilities
  - "Normal" conviction under S.53 + witness says *"I'm fairly sure I saw child porn on suspect's screen"*
    - => implies go-to-jail for much longer!
    - Surely jury will be prejudiced?

Weird defence allowed

- *"Where, in those specific circumstances, the person found guilty of the section 53 offence could show that the protected information did* ***not*** *contain an indecent photograph or pseudo-photograph of a child they could be liable to no more than a maximum term of two years."*

How is this supposed to work !!!!

- It's either decrypted or it ain't?
- Intended to penalise late compliance at time of trial?
  - but wholly innocent person anyway could be imprisoned for 2 years for innocuous information
  - e.g. defences own forensics recovered key later, still could be guilty of S.53!

Summary: potential harmful effects of activating RIPA Pt.3

- Stimulate an arms-race which law enforcement cannot win
  - UK becomes proving ground for steganography and VAMPware
  - bad guys have incentive for causing mayhem through VAMPware cases for "cover"
- Suppress and deter honest users from implementing reasonable security precautions commensurate with contemporary threats
  - When/if strong-authentication/encryption to access user data becomes widespread, highly likely to generate miscarriages of justice
  - drive policy towards "authentication-escrow"?
  - …maybe use your Home Office ID card to log into everything?
- S.49 has no effective value beyond common-law evidence rules, except for intimidatory effect during interrogations
  - burden-of-proof not workable either way