Technical Limits on ISP Action

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Musicians, fans and online copyright
London, 19th March 2008

Controlling bandwidth

- Most ISPs badge ADSL products from companies with DSLAMs in exchanges
- This means they pay for bandwidth to rest of the Internet AND to their customers
- Uneconomic to let customers max-out links on 24 x 7 basis (and market very price-sensitive)
  - so charge for usage (nGB/month)
  - and/or traffic shape to slow down p2p streams
    - proprietary devices use DPI and heuristics

Content blocking

- Most UK consumer ISPs implement content blocking for most customers for most sites on the IWF list of child abuse image sites
- Some do better than “most” !
- Systems are generally HTTP (and DNS) protocol specific and cannot be scaled or adapted for more generic blocking purposes
- So irrelevant, but mentioned for completeness!

How is illegal file-sharing detected ?

- Third party companies monitor the web and detect unauthorised JPGs, MP3s, AVIs, etc
  - they also monitor torrents (etc) for what is available on peer-to-peer systems
- A test access is made to ensure authentic
- IP address of server can be tracked to ISP
- ISP is in a position to identify their customer – what happens next varies…

Detecting peer-to-peer

- Detecting P2P is a classic arms race
  - port numbers became meaningless long ago
  - but some "hiding" is quite distinctive to spot!
- Some of music industry (& Hollywood) want to monitor ISP backbones (to tackle "dark nets")
  - proprietary search for watermarks or fingerprints
  - expensive option (ISPs don't have backbones!)
  - easily defeated by end-to-end encryption
  - blocking is problematic because much legal content

The myth of the high-skill user

- The issue attracts people who don't understand software; or the Internet; or people! (or law)
  - hence belief that what works today will work tomorrow and that "the masses" will not have access to software countermeasures
- Encryption already being widely deployed and will prevent many existing "attacks"
- Next, and significant, challenge is effective measures against traffic analysis attacks

Technical Limits on ISP Action

http://www.lightbluetouchpaper.org

UNIVERSITY OF CAMBRIDGE
Computer Laboratory