DoS-resistant Internet Grand Strategy

Bob Briscoe

Jan 2006

why

- goal of group
  - to galvanise co-ordinated actions to make the Internet more resistant to denial of services attacks, without unduly blocking the emergence of innovative new applications of the Internet
- goal of writing a grand strategy
  - to lay out the space of possible activity across fields in order to prioritise
    - identify approaches that require less co-ordination between companies, industries, disciplines, jurisdictions
    - identify gaps where co-ordination unavoidable
    - identify approaches not worth pursuing
  - foster consensus, rather than “not invented here”
- audience
  - pt I discursive: internal, members, researchers
  - pt II conclusive: regulators, operators (regulatory, operations), vendors, researchers

BT

status

- structure
  - table of contents
  - bullet point content
- one review pass so far
- on group wiki (at LINX)
- recruited expert authors

multidisciplinary contents

• intro	• Malcolm Hutty (LINX)
• technical measures	• Bob Briscoe (BT) Mark Handley (UCL)
• economic & incentive-based measures	• Bob Briscoe (BT) Scott Shenker (ICSI & UCB)
• contractual measures	• Malcolm Hutty (LINX)
• regulatory measures	• Chris Marsden (Rand)
• commercial realities	• placeholder for all
• conclusions	• Malcolm Hutty (LINX)

technical measures

- various dimensions
  - improved operational practices (→BCP), equipment, architecture
  - mitigating attack force vs mitigating attack capability
  - attacks through vs on infrastructure
  - hooks to trace attacker identity
    - path symmetry, ingress interface, e2e connection address
- incremental deployment issues
- arms races
  - payload inspection vs cryptography
  - traffic analysis vs route anonymisers

economic & incentive-based measures

- pricing to increase the cost of attacks
- limits of economic approaches
  - value of attack >> cost
  - irrational attackers
- internal ‘pricing’ to drive throttles and policers
- incentivising the clean up of zombie hosts
- insurance – blurring of responsibility?

BT

contractual measures

- types of contract
  - end customer acceptable use policies
  - inter-provider contracts
    - various arrangements: pairwise, star-wise, overlay (edge-edge)
  - rights to prevent vs. after the fact sanctions
    - various sanctions: financial, reputation, service impairment
  - evidence by behaviour vs intent
- liability
  - paymasters, attack co-ord, vectors (zombie, carrier, OS, e-mail)
- attacker identification
  - responsibility for allowing anon access (radio access issues)
  - strength levels of identification

regulatory measures

- model AUPs/contracts? minimum requirements?
- enforceability across borders
- clarifying liability
  - paymasters, attack co-ord, vectors (zombie, carrier, OS, e-mail)
  - if enforceability let down by a country, is country liable?
- relevant law available in each jurisdiction
- extensible law to new forms of attack

BT

commercial realities

- place-holder for commentary on other sections
- some thoughts
  - value of fostering innovation vs preventing harm
  - feasibility of sanctions between mutually dependent peers
  - effect of virtualisation on all the above (inc simple wholesaling)

summary

- setting an agenda for action
- towards a DoS resistant Internet

getting involved

- edit on LINX WiKi

  access controlled: via Mark Handley <M.Handley@cs.ucl.ac.uk>
- first substantial draft from all authors: mid Apr
- snapshot
  <www.cs.ucl.ac.uk/staff/B.Briscoe/projects/dos/DoSGrandStrategy.html>

Bob Briscoe <bob.briscoe@bt.com>