DoS-resistant Internet Grand Strategy

technical and economic measures

Bob Briscoe

Jun 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

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

- operational best common practices
  - summary of BCP (separate thread of work)
- survey of proposed technical measures
  - described through a common reference model
  - guidance on avenues to avoid and most fruitful approaches
  - incremental deployment issues

BT

architectural component ideas
candidate list for the ‘network layer’

- **Network Ingress Filtering of Source Address Spoofing**
  - Defeating Denial of Service Attacks that Employ IP Source Address Spoofing., **IETF RFC2827**
- **Traceback**
  - S. Savage, D. Wetherall, A. Karlin, and T. Anderson “Practical Network Support for IP Traceback” *SIGCOMM (*2000)
- **Pushback**
  - R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker. Controlling High Bandwidth Aggregates in the Network. *Computer Communications Review*, 32(3), (July 2002)
- **Overlay Indirection Services**
  - A Keromytis, V Misra, D Rubenstein, “Secure Overlay Service” SIGCOMM (2002)
  - Secure Internet Indirection Infrastructure (i^3): K. Lakshminarayanan, D. Adkins, A. Perrig, and I. Stoica, “Taming IP Packet Flooding Attacks” *HotNets-II*, (2003)
- **Symmetric paths, client-server address separation, RPF checks, state set-up bit, nonce exchange, middlewalls**
  - M Handley and A Greenhalgh “Steps towards a DoS-resistant Internet architecture” FDNA (2004)
- **Re-feedback**
  - B Briscoe et al “Policing Congestion Response in an Internetwork using Re-feedback” SIGCOMM (2005)
- **Receiver-driven Capabilities**
  - T. Anderson, T. Roscoe, and D.Wetherall, “Preventing Internet enial of Service with Capabilities” *HotNets-II*, (Nov. 2003)
  - A. Yaar, A. Perrig, and D. Song, “SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks” *Symposium on Security and Privacy*, (2004)
  - X Yang et al, “DoS-limiting Internet architecture” SIGCOMM (2005)
- **Routing: off by default**
  - Hitesh Ballani, Yatin Chawathey, Sylvia Ratnasamyy, Timothy Roscoey, Scott Shenker “Off by Default!” HotNets (2005)
- **Traffic symmetry**
  - *C Kreibich et al, “***Using Packet Symmetry to Curtail Malicious Traffic”** *HotNets* (2005)

reference model: datagram comms

- intent: to describe all the architectural approaches within a common reference model
- simple high level abstraction of datagram comms
  - devices are the congestible resource
    - memory, network interface, disk, processor
  - abstracts essential features of device addressing
  - via explicit hierarchical addressing and implicit addressing of relays through routing process (incl DHT overlay)
  - includes multipath access to same resource

(controversial) guidance: “to be avoided”

- intend to include ‘obvious’ guidance
  - eventually for public policy audience
- avoid attack detection by what the payload says it is
  - app identifiers, port numbers
  - encryption & dynamic ports rule these out (cf. IP over Skype)
- avoid attack mitigation through hooks to real-world identity then manual intervention
  - not credible deterrent given DoS on the legal redress service
    - unless last resort for rare cracks in automated system
  - the global Internet lowest common denominator is anonymity
    - not even anonymity behind delegated traceability

(controversial) guidance

perhaps not so useful stuff

- attack detection by claimed source identifier
  - not without broad validation measures in place
- attack detection by tests of humanity
  - most human-usable services evolve to use by unattended computers
- attack detection by inferring attack signature from its behaviour
  - perhaps promising, but perhaps war-game not worth starting
- attack mitigation by requiring receiver permission
  - biggest targets are sites with most (anonymous) clients: server request floods
  - not useful unless receiver willing to randomly select clients
- mitigation by push-back beyond where congestion is being caused
  - requires uncongested router to validate push-back request
  - rather than validation through self-evident congestion caused
  - push-back requests become amplifying attack vector

(controversial) guidance: fruitful avenues

- attack detection & mitigation by how traffic behaves
  - ideally by congestion response
    given DoS is congestion, which is a valid network layer concern
- hooks in network for higher layers
  - state set-up flag, nonce exchange

BT

giving research guidance: with care!

- too early to rule out research avenues
  - but I'm going to follow my intuition anyway
- other researchers will follow their noses too
  - our advice is there to be ignored
    if assumptions can be circumvented
- defence in depth can be useful
  - but, then again, too many depths will stifle innovation

BT

economic & incentive-based measures

- pricing to increase the cost of attacks
  - more useful for interconnection charging than for retail user
  - to localise pain to the network allowing pain to be caused
  - internal ‘pricing’ to drive throttles and policers
  - encouraging the clean up of zombie hosts
  - alternatively, SLA-type penalties for breaking thresholds
- limits of economic approaches
  - value of attack to attacker >> cost to attacker, irrational attackers
    - both avoided if only use economic approach at interconnection
  - insurance blurs responsibility
    - even if localise pain to irresponsible networks
insurance tends to spread risk back to responsible networks
- re-ECN being progressed through IETF
  - basis for interconnection congestion charging
    - draft-briscoe-tsvwg-re-ecn-tcp-02
    - draft-briscoe-tsvwg-re-ecn-border-cheating.01

BT

recent working group activity
on technical-economic measures

- tactical approaches
  - BGP-based push-back
  - distributing DNS name server records
- strategic approaches
  - policing congestion response using re-feedback/re-ECN
  - state set-up flag

BT

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>