The Rising Tide: DDoS by Defective Designs and Defaults

Richard Clayton

UNIVERSITY OF CAMBRIDGE Computer Laboratory

SRUTI Workshop
San Jose CA
7th July 2006
Summary

- The D-Link DI-624 wireless router
- Other DDoS attacks on NTP servers
- More DDoS by Designs and Defaults
- Some generic themes
- Mitigation strategies
- Three ways to drown
- Conclusions
Poul-Henning Kamp

- Operates gps.dix.dk, stratum 1 NTP server
- Detected a DDoS attack in summer 2005
- Traffic was 3.19 million NTPv1 packets/day – 37 per second, 276256 distinct IP addresses
- Address pattern didn't look synthetic to me
- I located a UK resident (on static IP address) and tracked down the actual source
D-Link DI-624

- Source of traffic was DI-624 wireless router
- Obtains time from 50+ “stratum 1” NTP servers; random request every 30 seconds
- This is:
  - Far, far too often
  - Not appropriate for this class of device
  - In breach of the NTP server usage agreement
- NB: also overdoing it for DNS as well
Déjà vu all over again!

- 2000, University of Delaware: NetTime (NTP)
- 2002, Trinity College Dublin: Tardis (HTTP)
  - 420 requests/sec
  - 280,000 packets/sec!
- 2003, CSIRO Australia: SMC (NTP)
  - 80,000 packets/sec
Not just NTP

- **HOSTS.TXT**
  - Flash crowd when updated
- “F” Root Server
  - Brownlee et al found much traffic “broken”
- Netscape parallel downloading
- Mojo Nation overwhelmed by new users
- Dynamic DNS firms bars some D-Link devices
  - 10,000 (0.7% of 1.4 million) users = 25% traffic
Some common themes

- Service discovery
  - HOSTS.TXT, Mojo Nation
- Service access
  - NTP access by inappropriate systems
- Broken systems
  - DNS examples
- Plus some examples we learn to live with…
  - Netscape downloading, qmail multiple connections
Mitigation

• Distributed systems
  – Akamai works (but NTP system doesn’t)

• Out-of-band authorisation
  – CSIRO hid their NTP servers

• Education
  – Ever more clueless are writing software 😞

• Economics
  – Netgear settled for $375,000 & D-Link paid up too
Roles for ISPs and end-users?

- One approach to classic DoS/DDoS is to appeal to end-users to be hygienic, and to ISPs to disconnect the problem systems.
- End-users already running reputable code and updating is fraught (or not known about).
- No ISP is going to disconnect customers for running a DI-664 wireless router.
Three different ways to drown

• Flash crowd (L. Niven 1973)
  – Flash flood

• DoS/DDoS attacks by the wicked
  – Firehose

• Defective Designs and Default Settings
  – A slowly rising tide
  – Easy to ignore and doesn’t look dangerous
  – Countermeasures hard: Cnut I (994-1035)
Conclusions

- DDoS is not just zombies and bot-masters
- Similar failures continue to occur
- Victims tend not to notice for a long time
- Prevention mechanisms are weak
  - Education isn’t keeping pace with de-skilling
  - Economic incentives aren’t aligned
  - Legal solutions don’t work at network scale
- ISPs aren’t going to disconnect for “trivia”
The Rising Tide:
DDoS by Defective Designs and Defaults

Richard Clayton

http://www.lightbluetouchpaper.org/