Towards a Safer and More Robust Internet

Paul Vixie

Internet Software Consortium

August 2003

Success Disasters

- An idea can work well in a laboratory
  - "everything works as it should"
- And in testing
  - Small, controlled population
  - Limited patterns of use
- But fail in the broad public marketplace
  - "6" is not "60" is not "6000000"
  - Some malicious users or observers

Example Success Disasters

- Internet HOSTS.TXT file
  - Listed *every* internet-connected host of the day
  - Impossible to update, distribute, search at scale
  - Thus: DNS
- Classful Internet addressing
  - 100 “A”, 15000 “B”, 2000000 “C” networks
  - Impossible to create/maintain routing table
  - Thus: CIDR

More Examples

- 4 billion hosts allowed in IPv4
  - Not enough for each person on Terra
  - Definitely not enough for each cell phone
  - Thus: IPv6
- Networks operated by right-of-way owners
  - ISPs operate networks with leased assets
  - ISPs are more plentiful than Telcos
  - Thus: Internet Exchange Points

Even More Examples

- DNS protocol only allows 13 “root” servers
  - Unforeseen result of early IPv4 design choices
  - Host population demands vastly better coverage
  - Thus: *anycast*
- “Dot Com bubble” made many millionaires
  - Investors bought stock for resale, not dividends
  - Not every 20-something can be a millionaire!
  - Thus: crash and recession

Current Examples

- ISP operators must be experts in their field
  - Very little off the shelf technology or training
  - Vendor defaults are completely inappropriate
  - Thus: no admission control on customer traffic
- Host operators must be expert technologists
  - The Internet is full of dangerous places/people
  - PC and DSL market allows universal access
  - Thus: wide scale vulnerability and abuse

Problem Size and Scope

- The Internet doubled in size every 16 months from 1990 to 1999
- It's not even theoretically possible to map it
  - Or list vulnerable hosts (or fix them)
  - Or keep track of bad actors (or arrest them)
- The Internet has become a new ecosystem
  - Like biology: can be studied but not understood

Necessary Next Steps (1)

- Make infrastructure stronger, more robust
- Increase technology training by 1000x
  - Starting with students still in school
  - Including vendor engineers
  - Including ISP operators
  - Including home users
- Note: *any* country can still compete

Necessary Next Steps (2)

- Make “mirror” copies of important servers
  - *F.root-servers.org* now in Palo Alto, Madrid, Hong Kong, Los Angeles, New York City, Seoul, Auckland, Rome, Sao Paulo; coming soon to a few dozen more cities
- Add security to core Internet protocols
  - DNS was never secure, but it can be made so
  - ISC and others are very active in this area

Necessary Next Steps (3)

- Increase interconnection between ISPs
  - Stop depending on few/large intermediaries
  - Every metro needs its own IP exchange
  - Regulated carriers must be required to join
- Teach moral philosophy (ethics) in schools
  - Most Internet attacks are by children/teenagers
  - Damage done feels remote and theoretical
  - Many literally do not know right from wrong

Probable Next Steps

- All of this will cost more money
  - Increase size and training level at ISPs
  - Increase training available to home users
  - Increase interconnectivity between ISPs
- Internet usage fees are artificially low
  - Cost models are still immature
  - Many services are sold below *current* costs

Conclusions

- Biggest Internet engineering problem, ever:
  - *Scaling*
- Cyberspace and meatspace are now merging
  - *Problems in either are really problems in both*
- We've got to take all of this more seriously
  - *Internet vulnerability is a problem for society*
- It's not a sandbox or a laboratory any more
  - *Safety is more important than money, or fun*