Rethinking the design of the Internet: The end to end arguments vs. the brave new world

David D. Clark and Marjory S. Blumenthal

Presented by Josiah Matlack
End-to-end principles

• Application-level functions should not be built into the core of the network
  • Applications may have codependence
  • Applications may depend on a stable core

• Change to the core network should generally be avoided
  • Lower complexity
  • Generality
  • Efficiency
Reasons for change

• Lack of trust
  • Spam, network and application attacks (DoS)

• Increasing demand (need for stability)
  • Streaming audio/video
  • Netflix takes up 1/3 of all US bandwidth
  • Intermediate CDNs and caching of content

• Enhanced services provided by ISPs
  • Specialization of services versus innovation

• Imposition by third parties
  • Wiretapping, authoritarian governments, banned protocols
Reasons for change (cont.)

- Less tech-savvy users
What has changed?

- The rise of stakeholders (ISPs)
- Transition of government roles
- Motivations of the user base
- Tension between users
- Original principles were based on freedom and innovation
- Fine line between control and repression
- Decisions are more politicized
Interaction patterns

- Proof of identity vs. preservation of anonymity
  - Politics and free speech
  - Online voting
  - Online currency and purchases
  - Hardware/software identification (cookies, MAC address)

- Third party involvement
  - Government wiretapping, spying, censorship, taxation, etc.
  - ISP traffic regulation and load balancing
  - Private company intranets
  - Copyright law and material
Interaction patterns (cont.)

• Push and pull between third parties discovering information and users hiding it
  • Full access vs. traffic monitoring
  • ISPs claim the need for knowledge of usage patterns

• Forcible interaction
  • Trojans, DoS, spam
  • Endpoint security is insufficient

• Multiway communication (multicast)
  • One node cannot bring down network

• Need to interleave differing strategies
Technological strategies

- Modify the end node (status quo)
  - Compromise performance for correctness
  - Issues: ID is easy to fake
- Modify the core network
  - Hostile intent is likely, rather than application crutches
  - Firewalls, traffic filters and NAT already violate end-to-end principles
  - Issues: espionage is easier; impossible to filter traffic without looking at content
Technological strategies (cont.)

- Labels
  - Could label both content and users
  - Hard to enforce
  - Burden the content provider
  - Could be automated
  - Key building block of filtering schemes
  - Example: PICS system
  - Metadata tags on webpages
  - Port numbers
Technological strategies (cont.)

- Application-level services
  - Anonymizing message forwarders (Tor)
  - Mail server filtering
  - Content caching

- Trusted third parties
  - Certificate signing, time-stamping, simultaneous release
  - Store of verified user credentials
  - Public certification authorities
    - Performance issue
Non-technological challenges

• Law
  • Copyrights, transborder nature
  • After the fact, unlike technological prevention

• Vigilante self-regulation
  • MPAA, V-chip, BBB

• The price of anonymity
  • Anonymous, cyberbullying and accountability

• Government role has shrunk, as has funding
  • Antitrust law, consumer fraud, commercial code, taxation, FCC
Other considerations

- ISPs
  - Limited to core modification
  - Monopolistic claims and a lack of innovation
  - International/cultural differences

- Selective trust and selective access to data

- Rights and responsibilities of users
  - “Arms race” with third parties
  - Steganography and encryption
  - Private vs. public communication
Conclusions

• End-to-end principles
  • Flexible, general, open, and innovative
  • Clash with ISPs and governments
  • Expanding, less tech-savvy user base
  • Trust issues
  • Complex applications
  • Bad investments and short-term solutions
Questions?

- RSA and SSL
- CDNs
- SOPA/CISPA
- China’s firewall
- Protocols