

The Once&Future Internet – Avalon or The Waste Land

Jon Crowcroft

<http://www.cl.cam.ac.uk/~jac22>

Jon.crowcroft@cl.cam.ac.uk

The Net as was – TCP/IP&DNS

- Layered system – abstraction, modularity, flexibility
 - Addressing, Routing
 - Reliability&Robustness
 - Applications and Users
- Ease of Use
 - Naming (microsoft.com is easier than 128 bit addresses)
- Resource Pooling
 - Fair economics
- Note several design principles
 - Decentralised –
 - no single point of failure
 - Statistical multiplexing –
 - if you're not using it, others can
 - End-to-end design mantra – aka parsimony
 - Avoid kitchen sink or swiss army knie in lower layers
 - Postel Principle –
 - Be liberal in what you accept, conserviative in what you send

The Killer App (www)

- Hyperlinks
 - Unidirectional – surprise, but resilient!
- Markup
 - Extensible
- Transfer
 - Simple
- Still Decentralised (note well!)
- Still simple

Use and Abuse

- From 1992 on...bad guys & money
 - Worms, Viruses, Malware script kids
 - DDoS – blackmail
 - Piracy
 - Spam, Phish
- What next? The Cloud
 - Centralised
 - Advertising
 - Analytics
- Weaponized by NSA&GCHQ&5eyes

What Next?

- Recover original design principles in higher layers:
 - Can we build a decentralized cloud?
 - Can we build incentives to reduce abuse?
 - Including reduced advertising/analytics
 - Alternative Business models?
- Separately, can we recover an earlier design goal:
- Support distributed intelligence ?
- Where smarts of group are great than sum of parts
- Instead of being dumber than the dumbest member!

What next for sure?

- Internet of things
 - Home environment, security, entertainment, utilities
- Smart Cities (transport, energy)
- Mobile e-Health later, wellbeing sooner

- Vanishing interfaces
 - Gesture, context, habit

- Both these challenge us to provide really good privacy...
- ...in ever more private environments

Deep Dive in Decentralization

- Key is Highly Optimized Tolerance
 - Lots of local failures, less chance of global
 - Failure= fault or attach
 - May have residual emergent bad things – needs some care 😊
- Separating timescales
 - Online v. offline tasks:
 - Allocation v. use v. checking
 - Names, addresses, routes, link weights etc
- Hierarchies are your friend
 - Root allocation (prefixes, ASs, TLDs, Protocol IDs)
 - Distributed re-distribution

Address space

- IANA
 - (was Jon Postel – a man with a sense of humour – c.f. RFC1984)
 - Pre-fix or AS to ISP/Org
 - Post fix distributed via DHCP or net management or v6 autoconfig
 - Autonomous System manages set of prefixes under an AS
 - And a set of routing algorithms (and traffic engineering)
 - And relationships to other ASs/ISPs
 - E.g. peering, or customer or provider
- Routing -- interior and exterior - e.g. OSPF & BGP
- Decouples choice of algo in time from other AS choices
 - And from traffic engineering (to determine edge weights)
 - For internal or transit traffic

Name Spaces

- Originally users had to remember IPs(like phone numbers)
- 128.232.1.1 or 192.164.2.3 – not very friendly
 - So along came DNS
 - Then DNS update/dyn-dns and DNSsec
 - Distributed hierarchical name allocation
 - Hence www.microsoft.com or www.cl.cam.ac.uk
- Name = service – maps to address
 - Can change answer depending when and where asked
 - Rotaries/load balancers etc etc
- Decentralized to match organisations (not topology)
- Not connected to business relationships
- But can be offline checked....
- CAs

Resource Management

- Net wants to maximise revenue (TE/price)
- User wants to maximise utility (throughput/latency/power)
- Distributed solution
 - due to Frank Kelly et al in Cambridge &
 - implemented by Van Jacobson, Mike Karels at Berkeley &
 - Raj Jain and KK Ramakrishnan at DEC
- Users choose rates
- Net gives feedback
- Users adjust rates independently
- => Distributed optimisation!
- Can evolve – e.g. MPTCP and soon, TCPCrypt
- Better matches distributed TE

WWW

- URL, HTTP, HTML – key trick is URL
- URL = protocol + DNS server name + filename (sort of 😊)
 - But key trick is that a site points at another site,
 - but doesn't care if it moves or changes
 - No bi-directionality
- Scales!
- Eventually, offline, search/check fixes or removes broken links
- Or new content gets woven in
- Local, no global ownership or fixing.

Cloud

- Pile many racks in a warehouse
 - Fill with lots of commodity computers & disks &
 - some very expensive switches
 - Virtualize
 - So you can run any OS and multiple guests per h/w instance
 - Fine grain resource pooling...
- But centralized
 - Point of failure and attack (privacy loss)
 - Expensive for power consumption
 - Good for DDoS defense for SME but...
- Why lose all those Internet principles???

Decentralized Cloud (mist?)

- Everyone runs a VM+server in every device
 - Phone, home router, hub, car, bike
 - Put all content on it, and serve to who you approve
 - No adverts, no analytics, no cost
- What's needed?
 - Enough uplink speed/low latency
 - Given now (4G, WiFi, ADSL, fiber to home)
 - 2Mbps, 55Mbps, 100Mbps plenty
 - Enough storage
 - 35 years of my docs & mail & photo&video ==100Gbytes
 - 1 Terabyte == 50\$
 - Enough reachability & availability
 - IPv4 needs NAT traversal IPv6 coming
 - Multipath (via neighbours)
 - diversity

Security & resilience

- No servers = no passwords?
 - No, still need to crypt stuff in store (even during processing)
 - So need auth/crypt credentials
 - Multifactor (pass phrase, biometric + PICO)
 - PICO h/w + s/w uses context and proximity to allow access
- Backup and archives decentralized (across F&F) and crypted
 - redundant coded (c.f. eternity) for plausible deniability
 - Key recovery through resurrecting duckling protocol 😊
- Why would people buy this?
 - Free, secure, provenance tracking and auditing,
 - lower latency, less power hungry globally
 - No attention span deficit from eyeballing adverts
 - No intrusive analytics
 - But no money for cloud providers 😞

Summary and Conclusion

- Vision of the net was decentralized in all layers
- Has been messed up by cloud

- Could regain the original vision
- But not in interest of large providers
- But is in interest of citizens
- And possibly national cybersecurity too....

- Questions?

<http://nymote.org/>



Namaste!