# The Open Internet under Threat

Brian Trammell
ISOC Switzerland Chapter
27 November 2012

# Who am I?

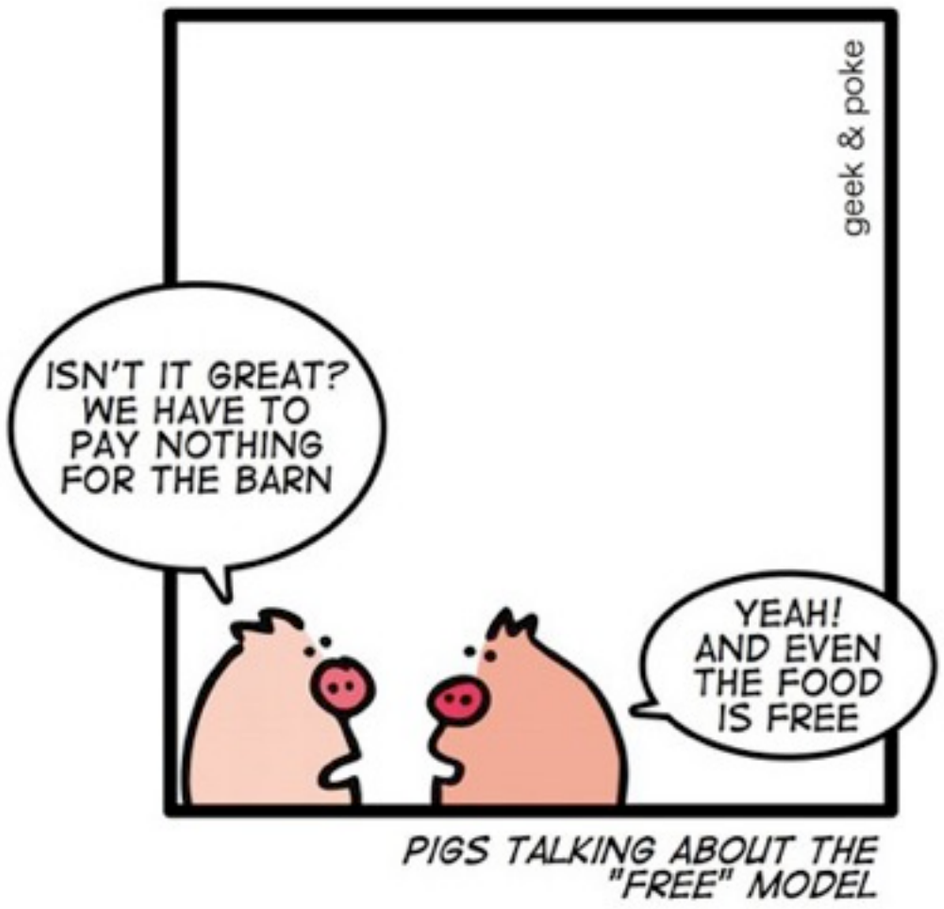
- Researcher, CSG, ETH Zürich
- Chair, IETF IP Performance Metrics (IPPM) and Managed Incident Lightweight Exchange (MILE) working groups
- Author of several RFCs on measurement (IPFIX) and cooperative security (INCH/MILE)
- Member, ISOC Switzerland Chapter
- Random guy off the street w/opinions that are his alone

# The Open Internet

- The End-to-End Principle: "Application-specific functions ought to reside in the end hosts of a network." (Saltzer *et al,* 1981)
- Decoupling of applications from transport allowed the Internet to displace POTS as *the network* and a platform for communication and innovation.
- This is a philosophy as much as it is an architecture.
- The network is notionally *open*, *neutral* and *stateless*.

# The Internet Today

- ~~Websites~~ → Apps
- ~~Open protocols~~ → closed platforms.
- Growth of free/ freemium model




http://geekandpoke.typepad.com // CC-BY

# Skype

- Closed-source, closed-protocol VoIP/ videoconferencing application owned by Microsoft
- Business model: selling voice communication (easier to **monetize** on a closed protocol)
- Successfully addressed **technical** challenges to SIP/RTP-based VoIP (NAT traversal, selective QoS)
- Largest single provider of cross-border voice in the world: 13% of int'l call volume in 2010.

# Twitter

- Public short message protocol built on a closed distributed database and proprietary API.
- Business case: promotion, advertising, graph mining (easier to **monetize** than a distributed protocol)
- Ecosystem of applications disrupted by API changes.
- Single entry point: single point of failure, single point of (**political**) control.
- Who has access to identity? Who can block tweets?

# Google

- Large advertising company, application service provider, mobile OS developer, and browser vendor.
- Control of two sides of the connection (CDN/ASP, device/browser) allows innovation:
  - SPDY: a faster replacement for HTTP, addresses flow-concurrency issues in modern applications.
- Control of two sides of the connection allows capture:
  - We have to trust Google to not be evil.

# Threats

- **Economic**: a closed network is more easily profitable.
- **Sociopolitical**: authority over the network necessary to protect citizens from harm or objectionable activity, enforce the law, and/or ensure state security.
- **Technical**: maintaining an open network in the face of growth, diversity, and service evolution is hard.

# Economic threats

- Closed protocols easier to monetize than open ones
  - e.g. Twitter, Facebook: **communication protocols** built atop proprietary distributed databases
- The carrier/provider split is a difficult business model
  - Operator margins are thin: value-added capture (e.g. "triple play")
  - Content providers find it hard to get paid

# Sociopolitical threats

- state security: intercept for counterterrorism and political surveillance, censorship of politically sensitive material
- citizen security: intercept for law enforcement, censorship of objectionable or illegal material
- copyright security: protection of publisher rights
- (...and old-school bureaucratic avarice: ITU-T)

# Technical threats

- IPv4 address exhaustion
- Network address translation
- IPv6 transition
  - The three above are deeply interrelated.
- Misuse and misuse prevention
  - SMTP/IMAP/POP replaced by Gmail, private message services like Facebook

# The Dystopian Future

- Irreplaceable services become de facto monopolies.
- Captured networks kill innovation.
    - What would the Web be like, if you needed a Web license to use or develop Web applications?
- Centralization of control leads to centralization of architecture: the end of end-to-end.

# Solutions?

- I'm mainly just here for structured complaint.
- Raising awareness:
  - We shouldn't trade fundamental flexibility for specific applications we like at the moment.
  - "If you're not paying for a service, you're the product"
- We need to frame the problem for specific audiences.

# Divide and Solve

- How to address each class of threat:
- **Economic**: Improve open-net business models?
- **Technical**: Simplify the core: get IPv6 deployed.
- **Sociopolitical**: ???
- Let's discuss: brian@trammell.ch