Reflections on Internet Transparency

draft-iab-net-transparent-00.txt

IAB Technical Plenary
November 9, 2006
San Diego, California
http://www.drizzle.com/~aboba/IAB/IAB-Transp.pdf

Questions

- How has the thinking on Internet Transparency evolved over the years?
  - What core tenets still guide us?
  - What new insights have we developed?
- What transparency issues have not received enough attention?
  - Additional transparency barriers being encountered
  - Potential transparency barriers

Some Documents Relating to Internet Transparency

- IAB Documents
  - RFC 1958: “Architectural Principles of the Internet”
  - RFC 2775: “Internet Transparency”
  - RFC 3724: “The Rise of the Middle and the Future of End-to-End”
- DARPA New Arch Project
  - New Arch: Future Generation Internet Architecture, http://www.isi.edu/newarch/iDOCS/final.finalreport.pdf
  - Tussle in Cyberspace: Defining Tomorrow’s Internet
  - http://www.acm.org/sigs/sigcomm/sigcomm2002/papers/tussle.pdf
- Other Documents
  - RFC 4084: Terminology for Describing Internet Connectivity

Previous IAB Statements

- RFC 1958, Section 2:
  - In very general terms, the community believes that the goal is connectivity, the tool is the Internet Protocol, and the intelligence is end to end rather than hidden in the network.
- RFC 3724, Section 4.1.1:
  - One desirable consequence of the end-to-end principle is protection of innovation. Requiring modification in the network in order to deploy new services is still typically more difficult than modifying end nodes.
- RFC 2775 Section 6:
  - Although the pure IPv6 scenario is the cleanest and simplest, it is not straightforward to reach it. The various scenarios without use of IPv6 are all messy and ultimately seem to lead to dead ends…. deployment of IPv6… is also messy but avoids the dead ends.

Concepts from the DARPA New Arch Project

- “Oblivious Transport”
  - A network that does not filter or transform the data that it carries may be said to be "transparent" or "oblivious" to the content of packets.
- “Tussle” (from “Tussle in Cyberspace”):
  - [The process by which] different parties adapt the [Internet’s] mix of mechanisms to try to achieve their conflicting goals, and others respond by adapting the mechanisms to push back.

Some Observations

- The IAB's past statements on transparency remain relevant today.
- The "tussle" that lead to a reduction in Internet transparency continues.
  - There is no architectural "fix" that can restore oblivious transport while satisfying the interests of all parties.
  - While transparency provides great flexibility, it also makes it easier to deliver unwanted as well as wanted traffic (see Unwanted Traffic Workshop Report).
  - IPv6 transparency is not pre-ordained, but represents an ideal that will require ongoing effort.
  - DNSSEC deployment may be hampered by transparency barriers.
- RFC 4084 provides a framework for conversation between providers and consumers.

Thoughts From RFC 4084

- On “Full Internet Connectivity”
  - “Filtering Web proxies, interception proxies, NAT, and other provider-imposed restrictions on inbound or outbound ports and traffic are incompatible with this type of service. Servers ... are typically considered normal. The only compatible restrictions are bandwidth limitations and prohibitions against network abuse or illegal activities.”
- On disclosure obligations
  - “More generally, the provider should identify any actions of the service to block, restrict, or alter the destination of, the outbound use (i.e., the use of services not supplied by the provider or on the provider's network) of applications services.”

Transparency Issues

- Application Layer Gateways
  - No such thing as a “transparent ALG”.
- DNS Namespace Mangling
  - Recursive forwarders modifying responses are incompatible with DNSSEC.
- Load Balancing and Redirection
  - Techniques such as Anycast and reverse NAT create transparency issues.
- IPv6 Address Restrictions
  - IKEv2 tunnel mode clients may only obtain a single IPv6 address
  - Providers may not offer prefix delegation
  - Gateways may not support bridging and/or ND proxy
- Application filtering in the core
  - Applications may be blocked without consent of the edge
- QoS
  - QoS may be used to restrict deployment of new applications

Next Steps

- Strawman -01 draft:
  - http://www.drizzle.com/~aboba/IAB/draft-iab-net-transparent-01.txt
- Comments solicited!
  - Send feedback to iab@ietf.org

Background

Application Layer Gateways (ALGs)

- [RFC2775] Section 3.5: “If the full range of Internet applications is to be used, NATs have to be coupled with application level gateways (ALGs) or proxies. Furthermore, the ALG or proxy must be updated whenever a new address-dependent application comes along.”
- Issues:
  - ALGs represent an additional barrier to transparency above and beyond NAT.
  - ALGs create barriers to updating of existing applications as well as to deployment of new applications.
  - DNS ALGs represent a barrier to deployment of DNSSEC.
  - There is no such thing as a “transparent ALG”.

DNS Mangling

Principles

- The use of a unique root for the DNS namespace is essential.
- RFC 2826 Section 1.3: “The design and implementations of the DNS protocol are heavily based on the assumption that there is a single owner or maintainer for every domain”

- Issues
  - Recursive name servers and/or DNS forwarders may replace responses that indicate that a name does not exist with a name and an address record that hosts a web service.
    - Recursive forwarders modifying responses are incompatible with DNSSEC.

Load Balancing & Redirection

- Principle
  - Provided these services are well-implemented they can provide value; however, it is also possible for service to be disrupted.
- Issues
    - Reverse NATs may be used with IPv6 as well as IPv4
    - DNS re-direction may not properly determine locality
    - Misconfigured packet filters may result in improper shunting of traffic to overlay networks
    - Anycast service may not provide ‘oblivious transport’ in the face of routing changes

IPv6 Address Restrictions

- Principles:
  - RFC 2775 Section 5.1: “Note that it is a basic assumption of IPv6 that no artificial constraints will be placed on the supply of addresses, given that there are so many of them. Current practices by which some ISPs strongly limit the number of IPv4 addresses per client will have no reason to exist for IPv6.”
- Issues
  - IKEv2 may only allocate a single IPv6 address
  - Providers may not support prefix delegation
  - Gateways may not support bridging and/or ND proxy

Application Filtering

- Principles
  - Deployment of filtering at the edges provides customers with the flexibility to choose which applications they wish to block or allow, whereas filtering in the core may not permit hosts to communicate even when the communication would conform to the appropriate use policies of the administrative domains to which those hosts belong.
- Issues
  - Providers may not disclosure service terms and policies
  - Applications may be blocked without consent of the edge

Quality of Service

- Principle
  - The deployment of Quality of Service (QoS) technology on the Internet has potential implications for transparency since having better or worse QoS for a flow can result in making the Internet more or less oblivous to that flow.
- Issues
  - QoS may be used to restrict deployment of new applications

Feedback?