IAB Architectural and Policy Considerations for OPES...

and Wider Architectural Concerns

Open IAB Plenary

December 13, 2001

Salt Lake City IETF

The initial question, for OPES:

What are the architectural and policy considerations in chartering the OPES WG?

The wider questions:

What are the robustness, integrity, and privacy considerations for IETF protocols?

What is OPES (Open Pluggable Edge Services)?

- Server-authorized services (e.g., at the web cache):
  - Assembling personalized web pages;
  - Adding regional information to web pages.

- Client-authorized services:
  - Virus scanning;
  - Language translation.
  - Adaptation for limited bandwidth;

The history of chartering OPES:

- OPES at this IETF had its fourth IETF meeting.

- **Position papers:** “OPES would reduce both the integrity, and the perception of integrity, of communications over the Internet, and would significantly increase uncertainly about what might have been done to content as it moved through the network.” [CDT01, August 2001],

- **Email:** “OPES is deeply evil and the IETF should stay far, far away from this hideous abomination”. [ODell01, July 2001]

- The IAB got in on the loop after the third BOF: draft-iab-opes-01.txt, to be an Informational RFC.

The IAB document on OPES:

- It is a recommendation to the IESG in chartering OPES.

- The IAB draft does not have answers, it mostly describes issues that should be addressed.

- Somewhat like ”Security Considerations”: the WG has to convincingly argue that the issues have been addressed.

Questions raised in the IAB OPES document:

- (1) Is there **architectural benefit** to putting services inside the network (e.g., at the application-level web cache)?

Answer: yes.

Potential benefits:

– reduced delay to user;

– less wasted bandwidth, etc.

- (2) Do the architectural benefits outweigh the **costs**?

Potential costs:

- data integrity?
- difficulties in diagnosing failures?, etc.

- (3) Does OPES have an impact on the **application layer addressing** architecture?

Related work in the IETF:

RFC 3135: Performance Enhancing Proxies

Intended to Mitigate Link-Related Degradations

- Sections on:
  - Security Implications,
  - Fate Sharing,
  - End-to-end Reliability,
  - End-to-end Failure Diagnostics, etc.

So on to the more general issues:

- The IAB is planning on writing a document about general architectural considerations.

- We would like feedback from this group.

General architectural considerations:

- **Justifying the solution:**

  – Why are you proposing this solution, at this level of the architecture, instead of something else?

  – Interactions with other layers?

  – Would this restrict future developments? In what ways?

- **Long-term vs. short-term solutions:**
  - Is this proposal the best long-term solution?
  - If this is a short-term solution, what are costs?
  - Interactions with other short-term fixes?
  - Is there an exit plan?

- **General robustness concerns:**
  - Robustness to node failures.
  - Robustness to compromised nodes?
  - Robustness to imperfect or defective implementations?
  - Robust performance in a wide range of environments?

- **Balancing competing interests:**

  – Are you protecting the interests of other parties while you are protecting your own interests?

  – Are you protecting the interests of the future?

- **Tragedy of the commons?**
  - Will tragedy of the commons result if everyone implements this proposal?