

December 2001

Author: Sally Floyd (floyd@aciri.org) and Leslie Daigle (leslie@thinkingcat.com)

DEFINITION

Open Pluggable Edge Services (OPES) are services that would be deployed at application-level intermediaries in the network, for example, at a web proxy cache between the origin server and the client, that would transform or filter content. Examples of proposed OPES services include assembling personalized web pages, adding user-specific regional information to web pages, virus scanning, content adaptation for clients with limited bandwidth, language translation, among other applications.

BACKGROUND

The question of chartering OPES in the Internet Engineering Task Force (IETF) and the related controversy in the IETF community have raised to the fore several architectural and policy issues about robustness and the end-to-end integrity of data. One view expressed on OPES has been that “OPES is deeply evil and the IETF should stay far, far away from this hideous abomination.” Others have suggested that “OPES would reduce both the integrity, and the perception of integrity, of communications over the Internet, and would significantly increase uncertainty about what might have been done to content as it moved through the network,” and that therefore the risks of OPES outweigh any of the possible benefits.

TECHNICAL ISSUES

A natural first question is whether there is any architectural benefit to putting specific services inside the network (e.g., at the application-level web cache) instead of positioning all services either at the content provider or the end user. It seems clear that there can indeed be significant architectural benefit in providing some OPES services inside the network at the application-level OPES intermediary. For example, if some content is already available from a local or regional web cache, and the end user requires some transformation (such as adaptation to a limited-bandwidth path) applied to that data, provid-

ing that service at the web cache itself can prevent the wasted bandwidth of having to retrieve more data from the content provider, and at the same time avoid unnecessary delays in providing the service to the end user.

Further questions concern whether the architectural benefits of providing services in the middle of the network outweigh the architectural costs, such as the potential costs concerning data integrity, and whether an OPES service, designed primarily for a single retrieval action, has an impact on the application layer addressing architecture. OPES has raised a number of important questions regarding integrity, privacy, and security. In particular, it seems unavoidable that at some point in the future some OPES service will perform inappropriately (e.g., a virus scanner rejecting content that does not include a virus), and some OPES intermediary will be compromised either inadvertently or with malicious intent. Given this, it seems necessary for the overall architecture to help protect end-to-end data integrity by addressing, from the beginning of the design process, the requirement of helping end hosts to detect and respond to inappropriate behavior by OPES intermediaries. One of the goals of the OPES architecture must be to maintain the robustness long cited as one of the overriding goals of the Internet architecture. Given this, it has been recommended that the IESG require that the OPES architecture protect end-to-end data integrity by supporting end-host detection and response to inappropriate behavior by OPES intermediaries.

One-party consent, with one of the end-hosts explicitly authorizing the OPES service, must be a requirement for OPES to be standardized in the IETF. However, the one-party consent model by itself (e.g., with one of the end-hosts authorizing the OPES service, and the other end-host perhaps being unaware of the OPES service) is insufficient for protecting data integrity in the network. We also agree with others that, regardless of the security and authorization mechanisms standardized for OPES in the IETF, OPES

implementations could probably be modified to circumvent these mechanisms, resulting in the unauthorized modification of content. Still, this is true of many protocols considered by the IETF, and by itself should not represent a compelling reason not to standardize transport protocols, routing protocols, web caching protocols, or OPES itself. Instead, the infrastructure needs, as much as possible, to be designed to detect and defend itself against compromised implementations, and misuses of protocols need to be addressed directly, each in the appropriate venue.

Mechanisms such as digital signatures, which help users to verify for themselves that content has not been altered, are a first step towards the detection of the unauthorized modification of content in the network. However, in the case of OPES, additional protection to ensure the end-to-end integrity of data is desirable as well, for example, to help end-users to detect cases where OPES intermediaries are authorized to modify content, but perform inappropriate modifications.

If OPES is chartered, the OPES working group will also have to explicitly decide and document whether the OPES architecture must be compatible with the use of encryption by one or more ends of an OPES-involved session. If OPES was compatible with encryption, this would effectively ensure that OPES boxes would be restricted to ones that are known, trusted, explicitly addressed at the IP layer, and authorized (by the provision of decryption keys) by at least one of the ends. Compatibility with encryption would also help to prevent the widespread deployment of yet another set of services that, to benefit from, require one to keep one's packet contents in the clear for all to snoop.

ISOC POSITION

The Internet Architecture Board (IAB) has made the following recommendations about chartering OPES in the IETF:

An OPES framework standardized in the IETF must require that the use of any OPES service be explicitly authorized by one of the application-layer end-hosts (that is, either the content provider or the client). For an OPES framework standardized in the IETF, the OPES intermediary must be explicitly addressed at the IP layer by the end user. The overall OPES framework

needs to assist content providers in detecting and responding to client-centric actions by OPES intermediaries that are deemed inappropriate by the content provider. The overall OPES framework should assist end users in detecting the behavior of OPES intermediaries, potentially allowing them to identify imperfect or compromised intermediaries. If there exists a "non-OPES" version of content available from the content provider, the OPES architecture must not prevent users from retrieving this "non-OPES" version from the content provider. OPES documentation must be clear in describing these services as being applied to the result of URI resolution, not as URI resolution itself. All proposed services must define their impact on inter- and intra-document reference validity. The overall OPES framework must provide for mechanisms for end users to determine the privacy policies of OPES intermediaries.

Expanded Coverage from ISOC

In-depth articles, papers, links and other resources related to this topic are available from the ISOC site at <http://www.isoc.org/issues/005/>.

For More Information

Internet Architecture Board (IAB) : <http://www.iab.org>
Internet Engineering Task Force (IETF) : <http://www.ietf.org>
Draft IETF OPES Working Group: <http://www.ietf-opes.org/>

Examples in the News:

Proposed Web Protocol Sparks Tampering Fears
http://www.nwfusion.com/archive/2001/123819_08-13-2001.html?nw

Relevant IETF RFCs

Many IETF RFCs are relevant to the discussion of OPES. Visit the RFC Editor page at <http://www.rfc-editor.org/> for more information

About the Authors

Sally Floyd is a senior scientist at ICIR, the ICSI Center for Internet Research. Her research interests include congestion control in computer networks and the analysis of network dynamics. Among other activities, she is a member of the Internet Architecture Board.

Leslie Daigle is Director of Directory Research at VeriSign. Her primary area of focus is in Internet applications infrastructure, particularly naming and directories.

This paper is a condensed version of an IETF document edited by the authors.

About the Background Paper Series

Published by: The Internet Society • 1775 Wiehle Ave., Suite 102 • Reston, Virginia 20190 USA • Tel: +1 703 326 9880 • Fax: +1 703 326 9881 4, rue des Falaises • CH-1205 Geneva, Switzerland • Tel: +41 22 807 1444 • Fax: +41 22 807 1445 • Email: info@isoc.org • Web: <http://www.isoc.org/>