Open Pluggable Edge Services
Internet-Draft
Expires: March 26, 2007

M. Stecher
Secure Computing

September 22, 2006

Integrity, privacy and security in OPES for SMTP
draft-ietf-opes-smtp-security-01

Status of this Memo

Copyright Notice

Abstract

The Open Pluggable Edge Services (OPES) framework is application agnostic. Application specific adaptations extend that framework. Previous work has focussed on HTTP and work for SMTP is in progress. These protocols differ fundamentally in the way data flows and it turns out that existing OPES requirements and IAB considerations for OPES need to be reviewed with regards to how well they fit for SMTP adaptation. This document analysis aspects about the integrity of SMTP and mail message adaptation by OPES systems and privacy and security issues when the OPES framework is adapted to SMTP and lists

requirements that must be considered when creating the "SMTP adaptation with OPES" document.

Table of Contents

1. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1]. When used with the normative meanings, these keywords will be all uppercase. Occurrences of these words in lowercase comprise normal prose usage, with no normative implications.

2. Introduction

2.1 Differences between unidirectional and bidirectional application protocols

The IAB listed considerations for Open Pluggable Edge Services (OPES) in [2] and OPES treatment of those considerations has been discussed in [3]. Both documents make use of HTTP as an example for the underlying protocol in OPES flows, and focus on web protocols that have requests and responses in the classic form (client sends a request to a server that replies with a response of the same protocol within a single protocol transaction).

RFC 3914 [3] already indicates that other protocols may not fit in this context, for example in section 5.3: "Moreover, some application protocols may not have explicit responses...".

When using SMTP there are still client and server applications and requests and responses handled within SMTP, but email messages are sent by the data provider to the recipients (data consumers) without a previous request; on that abstraction layer, email delivery via SMTP is a unidirectional process and different from the previously handled web protocols such as HTTP. For example: Bypass has been defined for OPES so far by allowing the data consumer to request an OPES bypass by adding information to the application protocol request; the OPES system can then react on the bypass request in both the application request and response. For SMTP, the data consumer (email recipient) cannot request in-band that the OPES bypass handling of his/her messages.

The IAB considerations need to be revisited and special requirements may be needed for OPES handling of SMTP.

2.2 Non-standardized SMTP adaptations at SMTP gateways

A large number of email filters are deployed at SMTP gateways today; in fact all usecases listed in "OPES SMTP Use Cases" [6] are already deployed, often in non standardized ways. This opens a number of integrity, privacy and security concerns that are not addressed, and SMTP itself does not provide effective measures to detect and defend against compromised implementations.

OPES will most likely not be able to solve these issues completely, but at least might be able to improve the situaton to some extent.

2.3 Non-OPES issues of SMTP

The SMTP specifications [4] require that NDRs (Non Delivery Reports)

be sent to the originator of an undeliverable mail that has been accepted by an SMTP server. But it has become common practice for some sorts of mail (spam, worms) to be silently dropped without sending an NDR, a violation of the MUST statement of SMTP (see section 3.7 of [4]). While the user of a web protocol notices if a resource cannot be fetched, neither the email sender nor email recipient may notice that an email was not delivered. These kind of issues already exist and are not introduced by OPES.

2.4 Opportunities of OPES/SMTP to address some issues

Adding SMTP adaptations with OPES allows us to define a standardized way for SMTP gateway filtering, to offload filtering services to callout servers and address a number of the integrity, privacy and security issues. OPES offers methods to add OPES tracing information and to request bypass of filtering, and by that can make email gateway filtering a more reliable and standardized function. But OPES won't make email delivery via SMTP a reliable communication.

2.5 Limitations of OPES in regards to fixing SMTP issues

The biggest concerns when adding OPES services to a network flow are

that compromised, misconfigured or faulty OPES systems may change messages in a way that the consumer can no longer read them or that messages are not longer delivered at all.

Defining a standard way to mark mails that have been handled by OPES systems is fairly simple and does not require new techniques by SMTP gateways; they already today MUST leave tracing information by adding "Received" headers to mails. Therefore, recipients receiving broken mail have a fair chance of finding the compromised OPES system by using the trace information. There is still no guarantee, as the email have been broken in a way that makes even the tracing information unreadable; but the chance will be even better than with other protocols such as HTTP, because most email clients allow the user to display mail headers, while many browsers have no mechanism to show the HTTP headers that might include tracing info.

Email that cannot be delivered because a compromised OPES system prevented the delivery of legitimate mail, MUST result in a an NDR to be sent to the originator of the mail according to the SMTP specifications [4]. OPES should not be forced to fix the issue that NDRs are not reliable over SMTP.

3. Integrity, privacy and security considerations

3.1 Tracing info in OPES/SMTP

Tracing is an important requirement for OPES systems. Tracing information added to mails should follow a similar syntax and structure to that defined for OPES/HTTP in HTTP Adaptation with Open Pluggable Edge Services [5], and with the same guidelines as the SMTP specifications [4] define for the "Received" headers.

Trace information is then seen by mail recipients when the mails reach the recipient. Mail that cannot be delivered or that is blocked by the OPES service will either be rejected or cannot be delivered after it has been accepted by an SMTP server. In the latter case SMTP specifications [4] require that a NDR MUST be sent

to the originator; OPES requires that if a NDR is sent that the report MUST also contain information about the OPES system so that the sender gets informed. If an email is rejected, an OPES system MUST also include trace data in the SMTP response so that the originator can find out why and where the mail was rejected.

3.2 Bypass in OPES/SMTP

If a mail message was rejected or could not be delivered (and a NDR was sent), the originator of the message may want to bypass the OPES system that blocked the message.

If the recipient of a message receives a mail with OPES trace information, he may want to receive a non-OPES version of the message. Although there is no direct in-band request from the recipient back to the OPES system, the recipient can contact the sender and ask her to send the message again and to add a bypass request for the OPES system.

An OPES system MAY also define out-of-band methods to request a bypass, for example a web interface or an email message sent to it that results in the creation of a white list entry for the sender/ recipient pair. Examples for these out-of-band methods are email systems that keep a copy of the original email in a quarantaine queue and only send the recipient a block notification plus either a direct link, or a digest notification with the ability to retrieve the original message from quarantaine.

OPES MUST implement methods to request a bypass but there cannot be a guarantee that the bypass request will be approved. The security needs of the receiver or the receiver's network may demand that certain filters must not by bypassed (such as virus scanners for example). In general, the receiver should be able to configure a

client centric OPES system, i.e. the receiver should be able to indicate if he/she wants to receive a non-OPES version if the OPES service would result in rejection of the email.

Bypass requests could be added to the mail message or within the SMTP dialog. Bypass request data added to the mail message cannot bypass OPES services that operate on other SMTP dialog commands, which are sent before the mail message has been received (such as RCPT

commands).

Bypass request data sent at the beginning of a SMTP dialog may not reach the OPES system if intermediate SMTP relays do not support those bypass request commands and don't forward that information.

3.3 Compatibility with end-to-end encryption and signatures

End-to-end email encryption is a proven technology, although the majority of mails are still sent unencrypted. Encrypting and signing email messages is done on the content of the mail and would be transparent to SMTP. Encrypted mail messages can either be used to prevent OPES systems from inspecting or modifying the content, or it can be used as an explicit approval to filter the mail by the OPES system, if keys for decryption of the message are made available to the OPES system. Signing of mails can be used to trace whether content has been changed by intermediates.

There are security risks associated with storing cryptographic keys that must be addressed by implementors. Because this is not a simple task, it is only suggested as an option, not as a requirement for OPES/SMTP.

4. Protocol requirements for OPES/SMTP

In addition to other documents listing requirements for OPES, the discussion in this document implies specific requirements for designing and implementing SMTP adaptations with OPES:

- OPES Systems MUST add tracing headers to mail messages

- If an email message that has been accepted by an OPES system cannot be delivered, the non delivery report MUST include trace information of the OPES system.

- The OPES/SMTP specifications MUST define a bypass request option that can be included in mail messages.

- The OPES/SMTP specifications MUST define a bypass request option as an extension for SMTP dialogs.

5. IAB Considerations for OPES/SMTP

This section lists the IAB considerations for OPES [2] and summarizes how OPES/SMTP addresses them.

5.1 IAB Consideration (2.1) One-Party Consent

The IAB recommends that all OPES services be explicitly authorized by one of the application-layer end-hosts (that is, either the data consumer application or the data provider application). For OPES/SMTP this means consent of either the email message sender or the recipient.

The application agnostic architecture of OPES [7] requires that "OPES processors MUST be consented to by either the data consumer or data provider application" (OPES processor is the email gateway for OPES/SMTP). This cannot prevent the consent-less introduction of OPES processors by incompliant OPES entities.

5.2 IAB Consideration (2.2) IP-Layer Communications

The IAB recommends that OPES processors must be explicitly addressed at the IP layer by the end user (data consumer application).

This requirement has been addressed by the architecture requirements in section 2.1 of [7] and has been further clarified in section 2.2 of [3].

5.3 IAB Consideration (3.1) Notification

"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" [2].

For OPES/SMTP this translates into assistance for the email message sender to detect and respond to recipient-centric actions that are deemed inappropriate by the sender.

This has been addressed in Section 3.1 and by the second tracing requirements in Section 4. As discussed in Section 2.3 OPES/SMTP cannot prevent that NDRs are not sent or get blocked before reaching the sender of the original message.

5.4 IAB Consideration (3.2) Notification

"The overall OPES framework should assist end users in detecting the behavior of OPES intermediaries, potentially allowing them to

identify imperfect or compromised intermediaries" [2].

This is addressed in Section 3.1 and by the first tracing requirement in Section 4. It must be noted that some email systems do not make the email headers available to the end user although the headers belong to the payload that is transferred via SMTP. Building an OPES architecture with those email systems should be avoided or requires that the tracing information is made available to the end users in a different way.

5.5 IAB Consideration (3.3) Non-Blocking

"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" [2].

For OPES/SMTP this has been discussed in Section 3.2 and is addressed by the two bypass requirements of Section 4.

5.6 IAB Consideration Application Layer Addresses (4.x)

While "most application layer addressing revolves around URIs" (section 8 of [2]), SMTP uses email addresses, for which the considerations apply to some degree only.

The SMTP use cases document [6] includes a use case for Mail Rerouting and Address Rewriting. Alias and email list address resolution are standard function of an email gateway described in [4].

Translating the reference validity consideration regarding inter- and intra-document reference validity to SMTP, OPES services mapping internal to external email addresses MUST ensure to properly map addresses in all affected email headers.

5.7 IAB Consideration (5.1) Privacy

This consideration recommends that the overall OPES framework must provide for mechanisms for end users to determine the privacy

policies of OPES intermediaries.

The application agnostic part for OPES and has been discussed in section 10 of [3]. Email specific trace information that will be added to OPES/SMTP according to the requirements in Section 4 may raise additional privacy issues that MUST be added to the privacy policy description of the OPES system.

5.8 IAB Consideration Encryption

"If OPES was compatible with end-to-end 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" [2].

This has been discussed in Section 3.3.

6. Security Considerations

The document itself discusses security considerations of OPES/SMTP. General security threats of OPES are described in Security Threats for OPES [8]

Section 3.3 (about compatibility with end-to-end encryption) mentions that an OPES system could be approved to inspect encrypted mails by making keys available for decryption. It must be noted that an implementation of the decryption key handling raises security issues (such as availability and storage of cryptographic keys) that must be addressed by the implementer.

7. References

7.1 Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Floyd, S. and L. Daigle, "IAB Architectural and Policy Considerations for Open Pluggable Edge Services", RFC 3238, January 2002.

[3] Barbir, A. and A. Rousskov, "Open Pluggable Edge Services (OPES) Treatment of IAB Considerations", RFC 3914, October 2004.

7.2 Informative References

[4] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[5] Rousskov, A. and M. Stecher, "HTTP Adaptation with Open Pluggable Edge Services (OPES)", RFC 4236, November 2005.

[6] Stecher, M. and A. Barbir, "Open Pluggable Edge Services (OPES) SMTP Use Cases", RFC 4496, May 2006.

[7] Barbir, A., Penno, R., Chen, R., Hofmann, M., and H. Orman, "An Architecture for Open Pluggable Edge Services (OPES)", RFC 3835, August 2004.

[8] Barbir, A., Batuner, O., Srinivas, B., Hofmann, M., and H. Orman, "Security Threats and Risks for Open Pluggable Edge Services (OPES)", RFC 3837, August 2004.

Author's Address

Martin Stecher
Secure Computing Corporation
Vattmannstr. 3
33100 Paderborn
Germany

Email: martin.stecher@webwasher.com
URI: http://www.securecomputing.com/

Intellectual Property Statement

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.