Network Working Group
Internet-Draft
Expires: November 11, 2007

R. Shacham
H. Schulzrinne
Columbia University
May 10, 2007

HTTP Header for Future Correspondence Addresses
draft-shacham-http-corr-uris-00

Status of this Memo

Copyright Notice

Abstract

A large amount of email is non-personal, automated communication, such as newsletters, confirmations and legitimate advertisements. These are often tagged as spam by content filters. This type of correspondence is usually initiated by a transaction over the web, such as a purchase or signing up for a service. Therefore, we propose a new HTTP header to carry the addresses that may be used by the provider to correspond with the user. These may be email addresses, or those used in other protocols, such as SIP. This will

facilitate the automatic inclusion of these addresses in whitelists used for spam prevention.

1. Overview

A large amount of email is not personal communication, but rather automated. Examples of this include newsletters, confirmations of reservations, and legitimate advertisements that are sent as a result of a purchase. These are often tagged as spam by content filters because of their similarity to spam. Such communication is also sent as SMS text messages and recorded phone calls over the existing cellular or PSTN infrastructure, and it can be expected that, in the future, it will be sent over an IP-based infrastructure, in the form of audio, video and text, using the Session Initiation Protocol (SIP) [2]. Since such an IP-based infrastructure is far more vulnerable to spam as described in [9], the challenge of filtering out legitimate communication from spam will be faced there too.

Sender authentication in email through SPF [4], Sender ID [6] or DKIM [5] and with the SIP Identity header [7] makes it possible to accept communication based on whitelisting. However, the addresses of legitimate senders must be known beforehand. This is known as the "introduction problem". A user's whitelist or address book is often automatically populated by addresses to which he sends, but they will not contain the addresses of automated mailers to whom the user never sends. However, automated communication is usually initiated by a transaction over the web, such as a purchase or signing up for a free service. Such a transaction provides an opportunity to transfer the addresses that may be used to correspond in the future.

We propose an HTTP [3] header to carry a list of addresses that may be used by a provider of goods or services to correspond with the client in matters related to a transaction. The client (browser) may include these addresses in a whitelist for automatic acceptance in the future. The methods used to add to the whitelist and query it are outside the scope of this document.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1].

3. New Header Definition

We define a new HTTP header called "Correspondence-URIs". The header MUST be included only in a response. This header may contain any number of URIs, representing communication addresses of types such as email, SIP or "tel". The ABNF of this header appears below. The mailbox rule is a reference to RFC 1123 [12], the SIP-URI and SIPS-URI rules are a reference to RFC 3261 [2], and the telephone-uri rule is a reference to RFC 3966 [8]. This specification may be expanded to include other URI schemes.

```
Correspondence-URI = mailbox / SIP-URI
                   / SIPS-URI / telephone-uri
Correspondence-URIs = "Correspondence-URIs" HCOLON
              [Correspondence-URI *(COMMA Correspondence-URI)]
```

4. Security Considerations

This section discusses requirements and guidelines to ensure that this header is not used to force users to accept undesired communication.

4.1. Sending and Processing of the Header

While the requirements in this section specify how an HTTP server should use the header, they, more importantly, should be followed by an HTTP client (browser) so that it ignores the header when sent in an invalid way, since servers attempting to abuse the mechanism will not follow the requirements anyway.

This header MUST only be included in responses to POST requests. It is unlikely that a website should need to legitimately correspond with a user unless he has completed a transaction with the site, which would involve a POST request. Allowing the header in GET responses would leave the user open to constantly receive these headers, which would require his approval, as mentioned in the next section.

The header MUST only include addresses belonging to the same domain as the server. This limits the ability of organizations to provide third-party marketers or spammers access to their customer base.

A client MAY choose to accept this header only when the "https" [11] scheme is used. This would guard against the insertion of an unauthorized address into the header field.

4.2. Client Use of The Header

This section gives guidelines for how a client (browser) should use this header once it has accepted it in a response, ie. the requirements of the last section have been fulfilled. Since this is a matter of local policy, it is beyond the scope of this document to make any normative claims about this use.

This document does not specify any mechanism for whitelisting. It should be noted, however, that using the addresses returned in this HTTP header in a whitelist is only effective when senders are authenticated. This may be done through the Sender Policy Framework (SPF) [4], SenderID [6], or Domain Keys Identified Mail (DKIM) [5].

The browser should not include the addresses in the user's whitelist without user approval. A good way to get this approval is with a dialog box popping up at the time of receipt. He should be made aware of which addresses he is accepting. If he chooses not to include the addresses from a specific site in his whitelist, he should be given the option of not being asked the next time.

5. IANA Considerations

This document requires registration of a Message Header Field, as per [10].

Header field: Correspondence-URIs
Applicable protocol: http
Status: standard
Author/Change Controller: IETF
Specification document: this specification

6. References

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

[2] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Sparks, R., Handley, A., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[3] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[4] Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1", RFC 4408,

April 2006.

[5] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", February 2007.

[6] Lyon, J. and M. Wong, "Sender ID: Authenticating E-Mail", RFC 4406, April 2006.

[7] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", RFC 4474, August 2006.

[8] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

[9] Rosenberg, J. and C. Jennings, "The Session Initiation Protocol (SIP) and Spam", February 2007.

[10] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", RFC 3864, September 2004.

[11] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[12] Braden, R., "Requirements for Internet Hosts -- Application and Support", RFC 1123, October 1989.

Authors' Addresses

Ron Shacham
Columbia University
1214 Amsterdam Avenue, MC 0401
New York, NY 10027
USA

Email: shacham@cs.columbia.edu

Henning Schulzrinne
Columbia University
1214 Amsterdam Avenue, MC 0401
New York, NY 10027
USA

Email: hgs@cs.columbia.edu

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).