Network Working Group
Request for Comments: 2480
Category: Standards Track

N. Freed
Innosoft International, Inc.

January 1999

Gateways and MIME Security Multiparts

Status of this Memo

Copyright Notice

1. Abstract

This document examines the problems associated with use of MIME security multiparts and gateways to non-MIME environments. A set of requirements for gateway behavior are defined which provide facilities necessary to properly accomodate the transfer of security multiparts through gateways.

2. Requirements Notation

This document occasionally uses terms that appear in capital letters. When the terms "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" appear capitalized, they are being used to indicate particular requirements of this specification. A discussion of the meanings of the terms "MUST", "SHOULD", and "MAY" appears in RFC 1123 [2]; the terms "MUST NOT" and "SHOULD NOT" are logical extensions of this usage.

3. The Problem

Security multiparts [RFC-1847] provide an effective way to add integrity and confidentiality services to protocols that employ MIME objects [RFC-2045, RFC-2046]. Difficulties arise, however, in heterogeneous environments involving gateways to environments that don't support MIME. Specifically:

(1) Security services have to be applied to MIME objects in their entirety. Failure to do so can lead to security exposures.

For example, a signature that covers only object data and not the object's MIME labels would allow someone to tamper with the labels in an undetectable fashion. Similarly, failure to encrypt MIME label information exposes information about the content that could facilitate traffic analysis.

Composite MIME objects (e.g., multipart/mixed, message/rfc822) also have to be secured as a unit. Again, failure to do so may facilitate tampering, reveal important information unnecessarily, or both.

(2) Gateways that deal with MIME objects have to be able to convert them to non-MIME formats.

For example, gateways often have to transform MIME labelling information into other forms. MIME type information may end up being expressed as a file extension or as an OID.

Gateways also have to take apart composite MIME objects into their component parts, converting the resulting set of parts into whatever form the non-MIME environments uses for composite objects. Failure to do so makes the objects unusable in any environment that doesn't support MIME. In many cases this also means that multi-level MIME structures have to be converted into a sequential list of parts.

(3) Security services have to be deployed in an end-to-end fashion. Failure to do so again can lead to security exposures.

An integrity service deployed at something other than a connection end point means a region exists between the point where the integrity service is applied and the actual end point where object tampering is possible. A confidentiality service deployed at something other than a connection end point means a region exists where the object is transferred in the clear. And worse, distributed private keys are usually necessary whenever someone other than the originator applies an integrity service or someone other than the recipient removes a confidentiality service, which in turn may make theft of private key information a possibility.

All of these issues can be addressed, of course. For example, it may be possible to use multiple overlapping security services to assure that no exposure exists even though there is no end-to-end security per se. And keys can be distributed in a secure fashion. However, such designs tend to be quite complex, and complexity in a security system is highly

undesireable.

The preceeding three requirments are fundamentally in conflict: It is possible to satisfy two of them at once, but not all three at once.

In fact the conflict is even worse than it first appears. In most situations of this sort some sort of compromise is possible which, while not satisfying any of the requirements completely, does optimize some sort of average of all the requirements. Such a solution does not exist in this case, however, because many real world situations exist where any one of these requirements absolutely must be satisfied.

4. Solving the Problem

Since the previously described problem doesn't allow for a single solution the only viable approach is to require that gateways provide multiple solutions. In particular, gateways

(1) MUST provide the ability to tunnel multipart/signed and multipart/encrypted objects as monolithic entities if there is any chance whatsoever that MIME capabilities exist on the non-MIME side of the gateway. No changes to content of the multipart are permitted, even when the content is itself a composite MIME object.

This option must be provided so that entities behind the gateway that are capable of processing security multiparts and their MIME content will work properly. As mentioned previously, situations exist where application security requirements are absolute and must be accomodated, even when meeting them causes problems for other agents.

Exceptions are allowed only when there is no possibility of MIME support on one side of the gateway. For example, a gateway to a voice messaging system may have no useful way to represent a signed MIME object.

(2) MUST provide the ability to take apart multipart/signed objects, exposing the content (and in the process ruining the signature). When this approach is selected, gateways SHOULD NOT remove the signature. Instead, gateways SHOULD keep the signature intact and add to it a note that it will probably be invalid for checking the message contents, but may still be contain valuable information about the sender.

This option must be provided so that entities behind the gateway which are incapable of processing MIME will work properly.

(3) SHOULD provide the ability to select between the previous two options on per-user basis.

(4) MAY provide facilities to check signatures and decrypt encrypted content. Such facilities MUST NOT be enabled by default; the potential security exposure involved has to be assessed before such capabilities can be used.

(5) MAY provide facilities to sign and/or encrypt material passing from the non-MIME side to the MIME side of the gateway. Again, such facilities MUST NOT be enabled by default; the potential security exposure involved in the transfer of unsecured content within the application domain behind the gateway has to be assessed before such capabilities can be used.

A gateway which complies with the above requirements is considered to be security multiparts compliant.

5. Security Considerations

This entire document is about security.

6. References

[RFC-822] Crocker, D., "Standard for the Format of ARPA Internet Text Messages", STD 11, RFC 822, August, 1982.

[RFC-1847] Galvin, J., Murphy, S., Crocker, S. and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

[RFC-1123] Braden, R., Ed., "Requirements for Internet Hosts -- Application and Support", STD 3, RFC 1123, October 1989.

[RFC-2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, December 1996.

[RFC-2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, December 1996.

[RFC-2049] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples", RFC 2049, December 1996.

7. Author's Address

Ned Freed
Innosoft International, Inc.
1050 Lakes Drive
West Covina, CA 91790
USA

Phone: +1 626 919 3600
Fax: +1 626 919 3614
EMail: ned.freed@innosoft.com

8. Full Copyright Statement