Network Working Group
Request for Comments: 3097
Updates: 2747
Category: Standards Track

R. Braden
ISI
L. Zhang
UCLA

April 2001

RSVP Cryptographic Authentication -- Updated Message Type Value

Status of this Memo

Copyright Notice

Abstract

This memo resolves a duplication in the assignment of RSVP Message Types, by changing the Message Types assigned by RFC 2747 to Challenge and Integrity Response messages.

1. Introduction

RFC 2747 ("RSVP Cryptographic Authentication") [RFC2747] assigns RSVP Message Type 12 to an Integrity Response message, while RFC 2961 ("RSVP Refresh Overhead Reduction Extensions") [RFC2961] assigns the same value to a Bundle message. This memo resolves the conflict over RSVP Message Type 12 by assigning a different value to the Message Type of the Integrity Response Message in RFC 2747. It is believed that the protocol defined by RFC 2961 entered use in the field before the RFC's publication and before the conflicting Message Type was noticed, and that it may be easier to install new software in environments that have deployed the Integrity object than in those that have deployed the refresh reduction extension.

To simplify possible interoperability problems caused by this change, we also assign a new value to the Message Type of RFC 2747's Challenge message, to which the Integrity Response message is a reply.

2. Modification

Message Types defined in the RSVP Integrity extension [RFC 2747] shall be changed as follows:

- Challenge message has Message Type 25.
- Integrity Response message has Message Type 25+1.

3. Compatibility

Two communicating nodes whose Integrity implementations are conformant with this modification will interoperate, using Message Type 12 for Bundle messages and Message Types 25 and 26 for the Integrity handshake. A non-conformant implementation of the Integrity extension will not interoperate with a conformant implementation (though two non-conformant implementations can interoperate as before).

There is no possibility of an Integrity handshake succeeding accidentally due to this change, since both sides of the handshake use the new numbers or the old numbers. Furthermore, the Integrity Response message includes a 32-bit cookie that must match a cookie in the Challenge message, else the challenge will fail. Finally, a non-conformant implementation should never receive a Bundle message that it interprets as an Integrity Response message, since RFC 2961 requires that Bundle messages be sent only to a Bundle-capable node.

4. References

[RFC2747] Baker, F., Lindell, R. and M. Talwar, "RSVP Cryptographic Authentication", RFC 2747, January 2000.

[RFC2961] Berger, L., Gan, D., Swallow, G., Pan, P., Tommasi, F. and S. Molendini, "RSVP Refresh Overhead Reduction Extensions", RFC 2961, April 2001.

Security Considerations

No new security considerations are introduced beyond RFC 2747 itself and the compatibility issues above.

Authors' Addresses

Bob Braden
USC Information Sciences Institute
4676 Admiralty Way
Marina del Rey, CA 90292

Phone: (310) 822-1511
EMail: Braden@ISI.EDU

Lixia Zhang
UCLA Computer Science Department
4531G Boelter Hall
Los Angeles, CA 90095-1596 USA

Phone: 310-825-2695
EMail: lixia@cs.ucla.edu

Full Copyright Statement

Acknowledgement

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