Security Working Group
Internet Draft
Expire in six months

R. Thayer
June 1997

The ESP ARCFOUR Algorithm
<draft-ietf-ipsec-ciph-arcfour-00.txt>

Status of This Memo

This document is a submission to the IETF Internet Protocol Security (IPSEC) Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@tis.com) or to the editor.

This document is an Internet-Draft. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet-Drafts draft documents are valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.

Abstract

This draft describes the use of the ARCFOUR [Kaukonen] stream cipher algorithm to be used with the IPSec Encapsulating Security Payload [ESP].

Contents

1. Introduction

This draft describes the use of the ARCFOUR stream algorithm to provide confidentiality in conjunction with the IPsec ESP protocol [ESP].

This document assumes readers with the terms and concepts in [RFC-1825] and in [ESP]. This document follows the IPsec document framework described in [Framework].

ARCFOUR is described in detail in [Kaukonen].

1.1 Specification of Requirements

Interpret the keywords "MUST", "MUST NOT", "REQUIRED", "SHOULD", "SHOULD NOT", and "MAY" that appear in this document as described in [RFC-2119].

2. Cipher Algorithm

The cipher algorithm specified in this document is the ARCFOUR stream cipher.

Hardware implementations of this algorithm are expected to perform in the 5-20 megabyte per second range.

3. Cipher Key Specifications

The keys used with this cipher for ESP SHOULD be either 40 or 128 bits. All implementations must support 40 bit keys. All implementations SHOULD support 128 bit keys. The use of 40 bit keys SHOULD be limited due to known attacks against this algorithm with that key length.

The keying material passed from key management MUST be either 40 bits or 128 bits of key, passed as 5 or 16 bytes.

4. ESP Payload

The ESP packet payload contains only the actual payload data. No IV is required for this cipher.

5. Security Considerations

40 bit keys for ARCFOUR have been shown to be breakable. 128 bit keys should be used. 40 bit keys should only be used for exportable demonstration implementations.

As with any other encryption technology, one should examine the current literature for any new attack strategies discovered after this document was published.

6. Acknowledements

An earlier draft discussing the use of this cipher was published in **1996 by Caronni and Waldvogel, "The ESP Stream Transform", draft-**caronni-esp-stream-01.txt, September, 1996.

The ARCFOUR algorithm is described in [Schneier] and in the Internet Draft draft-ietf-cipher-arcfour-00.txt soon to be submitted by Kaukonen and Thayer.

The ESP protocol is more recently discussed in draft-ietf-ipsec-esp-04.txt.

The IPsec document framework is described in draft-ietf-doc-roadmap-00.txt.

7. References

[ESP] Atkinson, R., "IP Encapsulating Security Protocol (ESP)", Naval Research Laboratory, July 1995.

[Framework] The IP Security Document Roadmap, RFC-xxxx.

[Kaukonen] The ARCFOUR Stream Cipher, RFC-xxxx.

[RFC-2119] Bradner, S., "Key words for use in RFCs to indicate Requirement Levels", ftp://ds.internic.net/rfc/rfc2119.txt, March 1997

[Schneier] Schneier, B., "Applied Cryptography Second Edition", John Wiley & Sons, New York, NY, 1995. ISBN 0-471-12845-7

8. Editor's Address

Rodney Thayer
Sable Technology Corporation
246 Walnut Street
Newton, Massachusetts U.S.A.
617 332 7292
Fax 617 332 7970
<mailto: rodney@sabletech.com>