Network Working Group
Request for Comments: 4345
Category: Standards Track

B. Harris

January 2006

Improved Arcfour Modes for the Secure Shell (SSH) Transport Layer Protocol

Status of This Memo

Copyright Notice

Abstract

This document specifies methods of using the Arcfour cipher in the Secure Shell (SSH) protocol that mitigate the weakness of the cipher's key-scheduling algorithm.

1. Introduction

Secure Shell (SSH) [RFC4251] is a secure remote-login protocol. It allows for the use of an extensible variety of symmetric cipher algorithms to provide confidentiality for data in transit. One of the algorithms specified in the base protocol is "arcfour", which specifies the use of Arcfour (also known as RC4), a fast stream cipher. As [RFC4253] says, though, "Arcfour (and RC4) has problems with weak keys, and should be used with caution." These problems are described in more detail in [MANTIN01], along with a recommendation to discard the first 1536 bytes of keystream so as to ensure that the cipher's internal state is thoroughly mixed. This document specifies new cipher algorithms for SSH that follow this recommendation.

2. Conventions Used in this Document

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 [RFC2119].

3. Applicability Statement

Implementations of Arcfour are typically slightly faster and much smaller than those of any other encryption algorithm currently defined for SSH. This must be balanced, though, against the known security problems with Arcfour described in Section 5. In most cases, where speed and code size are not critical issues, the algorithms specified by [RFC4344] should be used instead.

4. Algorithm Definitions

The "arcfour128" algorithm is the RC4 cipher, as described in [SCHNEIER], using a 128-bit key. The first 1536 bytes of keystream generated by the cipher MUST be discarded, and the first byte of the first encrypted packet MUST be encrypted using the 1537th byte of keystream.

The "arcfour256" algorithm is the same, but uses a 256-bit key.

5. Security Considerations

The security considerations in [RFC4251] apply.

The discarded bytes of keystream MUST be kept secret and MUST NOT be transmitted over the network. The contents of these bytes could reveal information about the key.

There are two classes of attack on Arcfour described in [MIRONOV]. Strong distinguishers distinguish an Arcfour keystream from randomness at the start of the stream and are defended against by the algorithm defined in this document. Weak distinguishers can operate on any part of the keystream, and the best ones, described in [FMcG] and [MANTIN05], can use data from multiple, different keystreams. A consequence of this is that encrypting the same data (for instance, a password) sufficiently many times in separate Arcfour keystreams can be sufficient to leak information about it to an adversary. It is thus RECOMMENDED that Arcfour (either in the form described here or that described in [RFC4251]) not be used for high-volume password-authenticated connections.

6. IANA Considerations

The IANA has assigned the Encryption Algorithm Names "arcfour128" and "arcfour256" in accordance with [RFC4250].

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, January 2006.

[RFC4251] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, January 2006

[RFC4344] Bellare, M., Kohno, T., and C. Namprempre, "The Secure Shell (SSH) Transport Layer Encryption Modes", RFC 4344, January 2006.

[SCHNEIER] Schneier, B., "Applied Cryptography Second Edition: protocols algorithms and source in code in C", John Wiley and Sons, New York, NY, 1996.

7.2. Informative References

[FMcG] Fluhrer, S. and D. McGrew, "Statistical Analysis of the Alleged RC4 Keystream Generator", Fast Software Encryption: 7th International Workshop, FSE 2000, April 2000, <http://www.mindspring.com/~dmcgrew/rc4-03.pdf>.

[MANTIN01] Mantin, I., "Analysis of the Stream Cipher RC4", M.Sc. Thesis, Weizmann Institute of Science, 2001, <http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Mantin1.zip>.

[MIRONOV] Mironov, I., "(Not So) Random Shuffles of RC4", Advances in Cryptology -- CRYPTO 2002: 22nd Annual International Cryptology Conference, August 2002, <http://eprint.iacr.org/2002/067.pdf>.

[MANTIN05] Mantin, I., "Predicting and Distinguishing Attacks on RC4 Keystream Generator", Advances in Cryptology -- EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, May 2005.

Author's Address

Ben Harris
2a Eachard Road
CAMBRIDGE
CB3 0HY
UNITED KINGDOM

EMail: bjh21@bjh21.me.uk

Trademark Notice

"RC4" and "SSH" are registered trademarks in the United States.

Full Copyright Statement

Intellectual Property

Acknowledgement

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