Network Working Group
Internet Draft

Jeffrey I. Schiller
MIT

Expiration Date: January 2000

August 1999

Cryptographic Algorithms for the IETF

draft-ietf-saag-aes-ciph-00.txt

1. Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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 are draft documents 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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

2. Abstract

Today the IETF recommends, and in some places requires the implementation of the U.S. Data Encryption Standard (DES). This choice was made a number of years ago with the assumption that DES represented an unbreakable cipher. Recent work has shown this assumption to no longer be the case. Therefore this document discusses what alternatives and directions are available to the IETF.

3. Introduction

The design of encryption algorithms requires significant skill and training. It is beyond the scope and competence of the IETF to design such algorithms. Instead the IETF should and does make use of generally accepted algorithms in the industry. For many years the algorithm of choice for security was the U.S. Data Encryption Standard (DES). DES makes use of a 56 bit key and works on blocks of data which are 64 bits in length (8 bytes). The DES is a U.S. National Standard.

Recent work in the cryptographic community, particularly the construction of "Deep Crack" by the Electronic Frontier Foundation has made it clear that a 56 bit cipher is no longer acceptable for strong security. The Deep Crack engine can recover a DES key in as little as 24 hours.

In general a strong cipher, as used by the IETF, is one in which recovery of keys or enciphered data (without the key) is computationally infeasible with both existing technology, and technology that is projected to exist within approximately ten years of the selection of a suitable algorithm.

Because DES no longer meets this requirement, we need to select an alternative set of ciphers.

4. The Advanced Encryption Standard

The U.S. National Institute of Standards and Technology (NIST) has undertaken the Advanced Encryption Standard (AES) Project. This project called for cryptographers world-wide to submit ciphers to be considered as a replacement national (U.S.) standard for the DES. The AES project set out several criteria for consideration for the standard. Of particular interest to the IETF is that this new standard will operate on 128 bit blocks of data instead of the 64 bit blocks of data operated on by the DES and similar ciphers.

As of this writing NIST has selected 5 candidate from an original set of 15 submissions. However it may not be until sometime in 2000 or 2001 before a final algorithm, or set of algorithms is chosen.

Submitters to the AES process had to agree that they would make their proposed cipher available free of charge if their proposal was selected as the final standard. However they are not required to do so if they are not selected nor are they required to do so prior to the final selection.

However, several submitters have already stated their intention of making their cipher available for public use prior to the final NIST selection.

5. IETF Requirements

The Security Area Advisory Group (SAAG) of the IETF has considered the requirements for IETF selected ciphers. They are:

1. Strength: The IETF should standardize the use of "strong" ciphers which cannot be compromised either using today's best technology nor tomorrow's best technology (10 years, for example) based on reasonable projections of the evolution of computing technology.

2. Key Length of at least 128 bits: This criteria is related to the strength of the cipher. However even strong ciphers may support several different key lengths. For the use of the IETF in a "mandatory to implement" [1] cipher keys of at least 128 bits must be supported.

3. Is freely available: There should be no requirement for licensing or other intellectual property constraints.

4. Performance: Many IETF protocols have to operate at high speed. Cryptographic processing may need to be quick.

6. Meeting the Requirements

The obvious candidate from a security perspective is to use "Triple DES" (3DES). 3DES is the literal application of the DES cipher three time instead of simply once. Today the DES cipher has proven to be strong. Since its introduction in the 1970's it has been actively attacked without significant success. The primary problem with DES today is that its key length of 56 bits makes it vulnerable to the brute force search of all possible keys. This is what the Deep Crack engine performs.

However, invoking the DES algorithm three times increases the effective key length from 56 bits to 168 bits. This eliminates the brute force attack.

The advantage to this approach is that 3DES is fundamentally a

---

[1] In order to foster interoperation the IETF requires that at least one cipher be required to be implemented in a standards conforming implementation of a protocol.

version of DES and DES has been subject to over two decades of scrutiny by scores of cryptanalysts worldwide. No practical cryptanalytic attack has ever been published, leaving brute force as the only practical attack mechanism.

In March of 1999 at the Minneapolis IETF meeting, the consensus of the SAAG was that we should use 3DES as the mandatory to implement cipher. Working groups in the Security Area of the IETF are advised to update working documents to specify 3DES as the mandatory cipher.

7. Should there be an additional Cipher?

3DES has one significant problem, its performance is 3 times slower then DES and DES was never designed to be fast in software. The result is that our performance requirement is not being met in many compute-constrained environments.

At the SAAG meeting in July of 1999 at the Oslo IETF meeting we discussed the notion of specifying an additional mandatory cipher. 3DES would remain as the "safe but slow choice" and the additional cipher would primarily be used in areas where performance is an issue.

However, selecting an additional cipher is a difficult problem at this time. If the AES project had already concluded, our choice would be easy, we would choose the AES selected cipher. However the AES project has not yet completed, so we need to choose from the candidates.

Today there are 5 candidates; the first round AES finalists. We could easily choose one of these five.

However there was no consensus to do so at the meeting. For the time being, the IETF should not specify an additional mandatory cipher.

8. The Consensus

We did have consensus that we would likely choose an additional cipher at some future time, perhaps after the AES cipher is selected. There was pretty clear consensus that we should choose an AES cipher.

9. Choosing an AES Cipher

The AES program specifies that the successful cipher will operate on 128 bit blocks instead of the 64 bit blocks that DES (and 3DES) makes use of today. Supporting this will likely require implementers to change their code. Therefore we conclude that given the likelihood of the IETF specifying an AES cipher as mandatory, that implementers would be wise to consider the necessary changes to their software to support 128 bit ciphers in the future.

10. Issues Relating to Key Length

The AES program specifies a cipher that will operate on keys of length 128 bits, 192 bits and 256 bits. Although the IETF will likely only require the support of keys of 128 bits (which should be sufficient for the foreseeable future) it is likely that implementers will wish to make use of the longer key lengths possible with the AES.

We had a brief discussion at the SAAG meeting about the implications that arise from this. Specifically if we start using keys longer then 128 bits, we have to consider the impact that we have on the asymmetric key management ciphers and protocols that we are standardizing today. It is likely that these will need to be modified to provide additional cryptographic strength to match the additional cryptographic strength of an AES cipher using a key length of greater then 128 bits. [2]

---

[2] Frankly we can easily use longer keys while NOT changing the key exchange algorithms and key lengths. However we would not be offering the true security implied by the longer symmetric algorithm key length as the asymmetric portion of the protocol would become the weak link.

11. Conclusions

We have IETF consensus that we should phase out the use of ciphers whose key lengths are less then 128 bits. This implies that we should deprecate the use of DES when possible. For most protocols this means that we will mandate the use of 3DES for the foreseeable future. We are discussing the addition of a second mandatory to implement cipher, but do not yet have consensus on this.

Although we are deprecating the use of DES (and similar short key ciphers) we are not requiring that they must not be supported. DES and other algorithms can continue to be implemented in optional mechanisms and as optional additional ciphers.

12. Acknowledgments

The author would like to thank Marcus Leech for detailed reading and editing. This document reflects a discussion held at the Security Area Advisory Group meeting at the 45th IETF meeting held in Oslo during July of 1999. I would therefore like to acknowledge the members of the SAAG who contributed to this discussion.

13. Author's Information

Jeffrey I. Schiller
MIT Room E40-311
77 **Massachusetts Avenue**
Cambridge, MA 02139-4307 USA
Phone: +1 (617) 253-0161
E-mail: jis@mit.edu

Comments on this draft should be sent to: saag@lists.tislabs.com, the SAAG mailing list.