Date: Mon, 15 May 2000 09:51:09 -0700
From: "David A. McGrew" <mcgrew@cisco.com>
X-Mailer: Mozilla 4.5 [en] (WinNT; U)
X-Accept-Language: en
To: AESround2@nist.gov
Subject: Comments on AES from Cisco Systems, Inc.

Hello,

please find attached a PDF document, "Comments on the Advanced Encryption Standard".

thanks,

David

--
David A. McGrew, Ph.D.
Cisco Systems, Inc.
mcgrew@cisco.com

Comments on the Advanced Encryption Standard

David A. McGrew, Ph.D.
Cisco Systems, Inc.
170 West Tasman Drive, San Jose, CA 95134

May 15, 2000

This note provides comments on the Advanced Encryption Standard (AES) that reflect the perspective of Cisco Systems. We use cryptography in many forms and on many platforms, including in desktop and server applications, in cryptographic products (IPSEC and SSL), in support of secure network administration (Kerberos and SSH), and within our operating systems. We feel that our broad experience provides us with a good perspective to provide useful feedback.

Our first comment is that the process that NIST is using to develop the Advanced Encryption Standard is a good one. NIST has done a commendable job in developing, organizing, and executing the process. The openness of the process and the encouragement of discussion will no doubt contribute to the success of the standard. The rest of this note briefly reviews the issues of security, performance, key agility, modes of use, multiple ciphers within the specification, and specialized constraints, and provides recommendations based on our perspective.

Security

The most important aspect of AES is its security. Performance of the AES cipher on any particular platform should be a secondary consideration. We anticipate that our implementations of the AES cipher will become an inextricable part of the infrastructure of the future. Our customers will rely on the security of the cipher for decades to come.

Performance

While performance is not the primary goal of AES, it is worth noting that many candidates appear to provide security while delivering good performance across a variety of platforms. In particular, the operations of integer multiplication and bitwise rotation, which are costly to implement in hardware and FPGAs, appear to not be needed in order to provide security. On this basis, we recommend the adoption of a cipher that does not use these operations.

Key Agility

The ability of a cipher implementation to change keys quickly, often called 'key agility', is a performance requirement that is sometimes overlooked. Nevertheless, this requirement appears in many of the most important cryptographic implementations. Cryptographic protocols that support virtual private networking and electronic commerce often contain an aggregation point that simultaneously maintains cryptographic connections with a large number of peers simultaneously. We recommend the adoption of a cipher that provides key agility, to facilitate its usefulness in cryptographic aggregation points.

Modes of Use

The specification of the modes of use of AES is a worthwhile undertaking. We recommend that this specification effort be distinct from the AES effort, so that it gets the attention that it deserves and does not impede the advancement of the AES effort.

Multiple Ciphers within the Standard

We recommend that the specification contain only one cipher. To do otherwise would dilute the value of the standard.

To specify two ciphers rather than one would double the efforts of implementing, testing, and validating implementations of the standard. Given that many AES implementations will be undergoing formal security evaluations, this cost is significant. Also, any 'negotiation' protocol that can select between multiple ciphers, as might be used in case there are multiple ciphers specified in the standard, would also require implementing, testing, validating, and possibly evaluation.

In addition, the adoption of two ciphers within AES will halve the amount of cryptographic scrutiny that is brought to bear on the final cipher(s). It has been well observed that the cryptographic scrutiny on the current candidates has been stretched thin, and a 'multiple' standard will exacerbate this unfortunate trend.

Arguments in favor of a 'multiple' standard argue in favor of two notions: performance diversity and security diversity. The proponents of performance diversity favor a multiple standard in the hopes of providing better performance to some types of implementations. This argument has a faultly premise: that different types of implementations need not interoperate. In reality, interoperability is a concern across all types of implementations. E.g., smartcards do not always talk to smartcards, but may talk to a large aggregation device within a virtual private network.

The argument in favor of security diversity holds it important that a 'secondary' cipher be included in in the standard, in case a major security flaw might be found in the 'primary' cipher. This argument is attempting to solve future problems with current standards. It is unlikely that we would want to adopt the 'secondary' cipher without first reviewing its security with regard to new cryptanalytic methods. In the event that a major flaw is found in one of the AES finalists, this flaw would likely represent a significant advance in the body of knowledge of cryptanalysis. In this case, specifying a 'secondary' cipher in advance offers no advantage over selecting a new cipher in the event of a break. It is worthwhile to note that if a secondary cipher is specified, future standardization work will need to be done in order to mandate its use instead of the primary cipher. Furthermore, we are doubtful that any wholesale field upgrade of cipher systems (i.e., from AES primary to AES secondary) is possible. We also observe that, in order for this upgrade to be

effective, the standard would need to require the implementation of at least two ciphers, incurring the costs mentioned above.

NIST has expressed concerns about intellectual property issues, and has suggested that an 'alternate' cipher could be useful to protect against submarine patents. We respect NIST's concern over patent issues, and we are not opposed to the selection of an alternate. In the case that an alternate is selected, we recommend that the standard explicitly states that implementations are not required to implement the alternate.

Specialized Constraints

Lastly, we note that there may be issues that have been raised in the AES process that should be dealt with in other standards bodies. We are pleased with the leadership that NIST has shown in the AES effort, and we trust that many standards bodies will directly adopt AES. Nevertheless, there are cases with unusual constraints that cannot be solved with a block cipher suitable for general purpose use (e.g., high performance with low security, very high security). Such constraints should not be placed on the AES cipher, and such requirements are best delegated to more specialized standards bodies.

Conclusions

In summary, we recommend that security be the single major consideration, that the bitwise rotations and integer multiplication be avoided, that key agility be provided if possible, that the specification of modes of use be a separate effort, that the AES specify the implementation of a single cipher, and that highly specialized constraints be deferred to other standards bodies.

We conclude by thanking NIST for the open and constructive nature of the AES process. We look forward to participating in the rest of the process and working with NIST in the future.