Next Generation Encryption

April 2012
Last updated: October 2015

Contents

Introduction

Over the years, numerous cryptographic algorithms have been developed and used in many different protocols and functions. Cryptography is by no means static. Steady advances in computing and the science of cryptanalysis have made it necessary to adopt newer, stronger algorithms and larger key sizes. Older algorithms are supported in current products to ensure backward compatibility and interoperability. However, some older algorithms and key sizes no longer provide adequate protection from modern threats and should be replaced. This paper summarizes the security of cryptographic algorithms and parameters, gives concrete recommendations regarding which cryptography should be used and which cryptography should be replaced, and describes alternatives and mitigations.

Recommendations for Cryptographic Algorithms

The following table can help customers migrate from legacy ciphers to current or more secure ciphers. The table explains each cryptographic algorithm that is available, the operations that each algorithm supports, and whether an algorithm is Cisco's best recommendation. Customers should pay particular attention to algorithms designated as*Avoid* or *Legacy*. The status labels are explained following the table.

Table 1. Recommendations for Cryptographic Algorithms

Algorithm	Operation	Status	Alternative	QCR[1]	Mitigation
DES	Encryption	Avoid	AES	—	—
3DES	Encryption	Legacy	AES	—	Short key lifetime
RC4	Encryption	Avoid	AES	—	—
AES-CBC mode AES-GCM mode	Encryption Authenticated encryption	Acceptable NGE[2]	AES-GCM —	✓ (256-bit) ✓ (256-bit)	— —
DH-768, -1024 RSA-768, -1024 DSA-768, -1024	Key exchange Encryption Authentication	Avoid	DH-3072 (Group 15) RSA-3072 DSA-3072	— — —	— — —
DH-2048 RSA-2048 DSA-2048	Key exchange Encryption Authentication	Acceptable	ECDH-256 — ECDSA-256	— — —	— — —

DH-3072 RSA-3072 DSA-3072	Key exchange Encryption Authentication	Acceptable	ECDH-256 — ECDSA-256	— — —	— — —
MD5	Integrity	Avoid	SHA-256	—	—
SHA-1	Integrity	Legacy	SHA-256	—	—
SHA-256 SHA-384 SHA-512	Integrity	NGE	SHA-384 — —	— ✓ ✓	— — —
HMAC-MD5	Integrity	Legacy	HMAC-SHA-256	—	Short key lifetime
HMAC-SHA-1	Integrity	Acceptable	HMAC-SHA-256	—	—
HMAC-SHA-256	Integrity	NGE	—	✓	—
ECDH-256 ECDSA-256	Key exchange Authentication	Acceptable	ECDH-384 ECDSA-384	— —	— —
ECDH-384 ECDSA-384	Key exchange Authentication	NGE	— —	— —	— —

1. QCR = quantum computer resistant.
2. NGE = next generation encryption.

Avoid: Algorithms that are marked as *Avoid* do not provide adequate security against modern threats and should not be used to protect sensitive information. It is recommended that these algorithms be replaced with stronger algorithms.

Legacy: Legacy algorithms provide a marginal but acceptable security level. They should be used only when no better alternatives are available, such as when interoperating with legacy equipment. It is recommended that these legacy algorithms be phased out and replaced with stronger algorithms.

Acceptable: Acceptable algorithms provide adequate security.

Next generation encryption (NGE): NGE algorithms are expected to meet the security and scalability requirements of the next two decades. For more information, see Next Generation Encryption.

Quantum computer resistant (QCR): As of October 2015, there has been attention on quantum computers (QCs) and their potential impact on current cryptography standards. Although practical QCs would pose a threat to crypto standards for public-key infrastructure (PKI) key exchange and encryption, no one has demonstrated a practical quantum computer yet. It is an area of active research and growing interest. Although it is possible, it can't be said with certainty whether practical QCs will be built in the future. An algorithm that would be secure even after a QC is built is said to have *postquantum security* or be *quantum computer resistant (QCR)*. AES-256, SHA-384, and SHA-512 are believed to have postquantum security. There are public key algorithms that are believed to have postquantum security too, but there are no standards for their use in Internet protocols yet.

Cisco is committed to providing the best cryptographic standards to our customers. NGE still includes the best standards that one can implement today to meet the security and scalability requirements for network security in the years to come or to interoperate with the cryptography that will be deployed in that time frame. The biggest threat to crypto nowadays is another high-impact implementation issue, not a QC. So while we need to get smart about postquantum crypto, we need to do it in a way that doesn't create more complexity and less robustness. Cisco will remain actively involved in quantum resistant cryptography and will provide updates as postquantum secure algorithms are standardized.

Short key lifetime: Use of a short key lifetime improves the security of legacy ciphers that are used on high-speed connections. In IPsec, a 24-hour lifetime is typical. A 30-minute lifetime improves the security of legacy algorithms and is recommended.

Introduction to Cryptography

Cryptography can provide confidentiality, integrity, authentication, and nonrepudiation for communications in public networks, storage, and more. Some real-world applications include protocols and technologies such as VPN networks, HTTPS web transactions, and management through SSH.

Over the years, some cryptographic algorithms have been deprecated, "broken," attacked, or proven to be insecure. There have been research publications that compromise or affect the perceived security of almost all algorithms by using reduced step attacks or others such as known plaintext, bit flip, and more. Additionally, advances in computing reduce the cost of information processing and data storage to retain effective security. Because of Moore's law and a similar empirical law for storage costs, symmetric cryptographic keys must grow by 1 bit every 18 months. For an encryption system to have a useful shelf life and securely interoperate with other devices throughout its life span, the system should provide security for 10 or more years into the future. The use of good cryptography is more important now than ever before because of the very real threat of well-funded and knowledgeable attackers.

Cryptographic algorithms, in general, are divided into the following categories:

- **Symmetric key algorithms:** These algorithms share the same key for encryption and decryption. Examples include Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES).
- **Public key algorithms:** These algorithms use different, mathematically related keys for encryption and decryption. Examples include Digital Signature Algorithm (DSA) and the Rivest-Shamir-Adleman (RSA) algorithm.
- **Elliptic curve algorithms:** These algorithms function over points that belong to elliptic curves. Examples include Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA).
- **Hash:** These algorithms provide a constant-sized output for any input and their most important property is irreversibility.

The following section presents the recommended algorithms and key sizes for each category.

Next Generation Encryption

Next generation encryption (NGE) technologies satisfy the security requirements described in the preceding sections while using cryptographic algorithms that scale better. This document presents algorithms that are considered secure at present, the status of algorithms that are no longer considered secure, the key sizes that provide adequate security levels, and next generation cryptographic algorithms.

NGE Background Information

NGE offers the best technologies for future-proof cryptography and it is setting the industry trend. These are the best standards that one can implement today to meet the security and scalability requirements for years to come and to interoperate with the cryptography that will be deployed in that time frame.

The algorithms that comprise NGE are the result of more than 30 years of global advancement and evolution in cryptography. Each constituent component of NGE has its own history, depicting the diverse history of the NGE algorithms as well as their long-standing academic and community review. For instance, AES was named by the U.S. National Institute of Standards and Technology (NIST) but AES was not created by NIST. AES was originally called *Rijndael* and was created by two Belgian cryptographers. Additionally, ECDSA and ECDH have had fundamental contributions by cryptographers from around the world, including Japan, Canada, and the United States. In the end, NGE is composed of globally created, globally reviewed, and publicly available algorithms.

The following sections discuss the NGE algorithms in more detail.

Categories of Cryptographic Algorithms

There are four groups of cryptographic algorithms.

Symmetric Key

Symmetric key algorithms use the same key for encryption and decryption. Examples include 3DES and AES. 3DES, which consists of three sequential Data Encryption Standard (DES) encryption-decryptions, is a legacy algorithm. This designation means that 3DES provides a marginal but acceptable security level, but its keys should be renewed relatively often. Because of its small key size, DES is no longer secure and should be avoided. RC4 should be avoided too.

AES with 128-bit keys provides adequate protection for sensitive information. AES with 256-bit keys is required to protect classified information of higher importance.

Public Key

Public key algorithms use different keys for encryption and decryption. These keys are usually called the *private key*, which is secret, and the *public key*, which is publicly available. The private and public keys are cryptographically related. The private key cannot be derived from the public key. The private key can be used only by its owner and the public key can be used by third parties to perform operations with the key owner.

The RSA algorithms for encryption and digital signatures are less efficient at higher security levels, as is the integer-based Diffie-Hellman (DH) algorithm. There are subexponential attacks that can be used against these algorithms. To compensate, their key sizes must be substantially increased. In practice, this means that RSA and DH are becoming less efficient every year. DH, DSA, and RSA can be used with a 3072-bit modulus to protect sensitive information. Smaller DH, DSA, and RSA key sizes, such as 768 or 1024, should be avoided.

Elliptic Curve

Elliptic Curve Cryptography (ECC) is a newer alternative to public key cryptography. ECC operates on elliptic curves over finite fields. The main advantage of elliptic curves is their efficiency. They can offer the same level of security for modular arithmetic operations over much smaller prime fields. Thus, the relative performance of ECC algorithms is significantly better than traditional public key cryptography.

ECDH is a method for key exchange and ECDSA is used for digital signatures. ECDH and ECDSA using 256-bit prime modulus secure elliptic curves provide adequate protection for sensitive information. ECDH and ECDSA over 384-bit prime modulus secure elliptic curves are required to protect classified information of higher importance.

Hash

Hash algorithms are also called *digital fingerprinting algorithms*. They are irreversible functions that provide a fixed-size hash based on various inputs. Irreversibility and collision resistance are necessary attributes for successful hash functions. Examples of hash functions are Secure Hash Algorithm 1 (SHA-1) and SHA-256.

Message Digest 5 (MD5) is a hash function that is insecure and should be avoided. SHA-1 is a legacy algorithm and thus is adequately secure. SHA-256 provides adequate protection for sensitive information. On the other hand, SHA-384 is required to protect classified information of higher importance.

Hashed Message Authentication Code (HMAC) is a construction that uses a secret key and a hash function to provide a message authentication code (MAC) for a message. HMAC is used for integrity verification. HMAC-MD5, which uses MD5 as its hash function, is a legacy algorithm. Note that MD5 as a hash function itself is *not* secure. It provides adequate security today but its keys should be renewed relatively often. Alternatively, the NIST-recommended HMAC function is HMAC-SHA-1.

Security Levels

The following table shows the relative security level provided by the recommended and NGE algorithms. The security level is the relative strength of an algorithm. An algorithm with a security level of *x* bits is stronger than one of *y* bits if $x > y$. If an algorithm has a security level of *x* bits, the relative effort it would take to "beat" the algorithm is of the same magnitude of breaking a secure *x*-bit symmetric key algorithm (without reduction or other attacks). The 128-bit security level is for sensitive information and the 192-bit level is for information of higher importance.

Table 2. Security Strength by Algorithm

Algorithm	Security Level
AES-128 DH, DSA, RSA-3072 SHA-256 ECDH, ECDSA-256	128 bits
AES-192 SHA-384 ECDH, ECDSA-384	192 bits
AES-256 SHA-512 ECDH, ECDSA-521	256 bits

Cryptographic Algorithm Configuration Guidelines

After the review of NGE algorithms and recommendations on choosing cryptographic algorithms, it is worthwhile to review specific guidelines for security technology configuration. The guidelines in this section are by no means all inclusive. Cryptography is widely deployed in almost every technology; thus, it is impossible to provide exhaustive guidelines for every technology that employs cryptography.

IPsec VPN with Encapsulating Security Payload

Use the following guidelines when configuring IPsec VPN encryption with Encapsulating Security Payload (ESP):

- Do not use NULL encryption (esp-null).
- Use both an authentication algorithm (esp-sha256-hmac is recommended) and an encryption algorithm (esp-aes is recommended).

The following example shows a Cisco IOS Software or Cisco Adaptive Security Appliance (ASA) transform set configuration that uses 256-bit AES encryption and HMAC-SHA-256 authentication for ESP IPsec in tunnel mode:

```
crypto ipsec transform my-transform-set esp-aes 256 esp-sha256-hmac
```

Internet Key Exchange in VPN Technologies

Use the following guidelines when configuring Internet Key Exchange (IKE) in VPN technologies:

- Avoid IKE Groups 1, 2, and 5.
- Use IKE Group 15 or 16 and employ 3072-bit and 4096-bit DH, respectively.
- When possible, use IKE Group 19 or 20. They are the 256-bit and 384-bit ECDH groups, respectively.
- Use AES for encryption.

Caution: Administrators are advised to use caution regarding processing load when they choose IKE groups. Load depends on platform limitations. Some platforms may not support Group 15 or 16 in hardware, and handling them in the CPU could add significant load to the processor in lower-end products or multiple simultaneous IKE negotiation scenarios.

For Cisco ASA 5500 Series models, administrators are strongly advised to enable hardware processing instead of software processing for large modulus operations, such as 3072-bit certificates. Initially enabling hardware processing by using the **crypto engine large-mod-accel** command, which was introduced in ASA version 8.3(2), during a low-use or maintenance period will minimize a temporary packet loss that can occur during the transition of processing from software to hardware. For the Cisco ASA 5540 and ASA 5550 using SSL VPN, administrators may want to continue to use software processing for large keys in specific load conditions. If VPN sessions are added very slowly and the ASA device runs at capacity, the negative impact to data throughput is larger than the positive impact for session establishment.

The following example shows a Cisco IOS Software IKE configuration that uses 128-bit AES for encryption, pre-shared key authentication, and 256-bit ECDH (Group 19):

```
crypto isakmp policy 10
  encryption aes
  authentication pre-share
  group 19
```

The following example shows a Cisco IOS Software IKEv2 proposal configuration that uses 256-bit CBC-mode AES for encryption, SHA-256 for the hash, and 3072-bit DH (Group 15):

```
crypto ikev2 proposal my-ikev2-proposal
  encryption aes-cbc-256
  integrity sha256
  group 15
```

Not all product versions support SHA-256 or IKE Group 14, 19, 20, or 24. Recent releases of Cisco IOS Software and some other product version releases have incorporated support for some of these features.

Transport Layer Security and Cipher Suites

Many products are managed through a web interface using HTTPS. HTTPS uses SSL/Transport Layer Security (TLS) to encrypt communications. TLS is the successor of SSL and provides encryption, authentication, and integrity for web communications. TLS 1.2 is the current version. Where possible, TLS 1.2 is preferred over SSL 3.0, TLS 1.0, and TLS 1.1. TLS is also used in various Cisco products to provide VPN services.

Cipher suites are combinations of security algorithms that are used in TLS. When configuring products that support TLS, administrators are advised to use secure algorithms in the cipher suites of the TLS negotiation when possible. Some recommendations are as follows:

- Use 3072-bit certificates with cipher suites that include TLS_RSA_.
- Use 3072-bit DH or 256-bit or 384-bit ECDH and ECDSA with cipher suites that include:
  - TLS_DH_
  - TLS_ECDH_
  - TLS_ECDH_ECDSA or TLS_RSA_ECDSA
- Configure the negotiated TLS cipher suites to include AES-128 or AES-256 GCM as the encryption algorithms and SHA-256 or SHA-384 for the hashes. The negotiated cipher suites should include:
  - WITH_AES_128_GCM_SHA256 or WITH_AES_256_GCM_SHA384
  - WITH_AES_256_GCM_SHA256 or WITH_AES_256_GCM_SHA384

  Alternatives are:
  - WITH_AES_128_CBC_SHA256
  - WITH_AES_256_CBC_SHA256

Browsers should support the preceding cipher suites, as should the HTTP server or SSL VPN concentrator. However, not all product versions support the preceding cipher suites. Support is progressively added.

Acknowledgments

Panos Kampanakis (pkampana[at]cisco[dot]com)
Security Intelligence Operations

David McGrew (mcgrew[at]cisco[dot]com)
Cisco Fellow, Corporate Security Programs Office (CSPO)

Jay Young-Taylor (jyoungta[at]cisco[dot]com)
Escalation Support Engineer, Cisco Services

Wen Zhang (wzhang[at]cisco[dot]com)
Escalation Support Engineering, Cisco Services

Lonnie Harris (lonnieh[at]cisco[dot]com)
Test Engineer, Global Government Solutions Group (GGSG)

References

NIST SP 800-131A, B, and C
http://csrc.nist.gov/publications/PubsSPs.html

NIST Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (SP800-131A)
http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

IANA Transport Layer Security (TLS) Parameters
http://www.iana.org/assignments/tls-parameters/tls-parameters.xml#tls-parameters-3

IANA Internet Key Exchange (IKE) Attributes
http://www.iana.org/assignments/ipsec-registry

Appendix A: Minimum Cryptography Recommendations

The following table lists recommended cryptographic algorithms that satisfy minimum security requirements for technology as of October 2015.

Table 3. Recommended Minimum Security Algorithms

Operation	Recommended Minimum Security Algorithms
Encryption	AES-128-CBC mode
Authentication	RSA-3072, DSA-3072
Integrity	SHA-256
Key exchange	DH Group 15 (3072-bit)

This document is part of Cisco Security Research & Operations.

Back to Top

Information For
Small Business
Midsize Business
Service Provider

Industries

Marketplace

Contacts
Contact Cisco
Meet our Partners
Find a Reseller

News & Alerts
Newsroom
Blogs
Field Notices
Security Advisories

Technology Trends
Cloud
Internet of Things (IoT)
Software Defined Networking (SDN)

Support
Downloads
Documentation

Communities
DevNet
Learning Network
Support Community

Video Portal

About Cisco
Investor Relations
Corporate Social Responsibility
Environmental Sustainability
Trust and Transparency Center
There's Never Been A Better Time

Careers
Search Jobs
We Are Cisco

Programs
Cisco Designated VIP Program
Cisco Powered
Financing Options

Contacts | Feedback | Help | Site Map | Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks