Technology Paper

128-Bit Versus 256-Bit AES Encryption

Practical business reasons why 128-bit solutions provide comprehensive security for every need

Background

There is some confusion around the market for full disk encryption (FDE) products. Seagate Technology LLC has introduced a line of products that offer 128-AES encryption. Some software and competitive hardware products offer 256-AES encryption. The question is: Are the 256-AES product offerings better than comparable 128-AES products?

To answer that question, it's necessary to define "better." Given that we are talking about protecting data at rest, it's reasonable to define better to mean "significantly more difficult for unauthorized parties to access the protected data."

The short answer is "no." Exhaustive key search techniques on a key space of 128 bits, using the latest streamlining processes, require resources (MIPS, memory, power and time) many orders of magnitude beyond current capabilities. Any unseen breakthroughs would most certainly apply to 256-bit as well as 128-bit.

(A brief explanation of the terms 128-AES and 256-AES: AES is a symmetric key algorithm. AES encrypts and decrypts data in 128-bit blocks, using 128-, 192- or 256-bit keys. AES nomenclature for the different key sizes is AES-x, where x is the key size.)

To understand an attacker's path to data, we need to describe the system. The primary components of a data-at-rest security system are the authentication module and the encryption engine.

Enterprise applications, of course, include many management tools that vary by each installation. These tools may be used to generate or escrow passwords and keys and to track and establish users and their digital identities. This paper will not delve into these management tools. Rather, the focus will be a discussion on the strength of security of the core components, namely the authentication module and the encryption engine.

Authentication Module

It wouldn't make sense for someone to invest a million dollars on security measures for doors and windows and all other entry points in their home, but use a pass code of "1234" as the combination to open the front door.

This exemplifies why maximizing security involves combining strong access controls to the system with strong secure processes for handling and processing data and secrets.

Remember the adage: A chain is only as strong as its weakest link.

While the opening statement of this paper suggested confusion over encryption key length, the latter portion of this paper should convince you that the encryption engine strength should be of least concern, given the ingredients of the encryption engines in question. With these encryption engines in place, the real key (no pun intended) to strong security is to assure that the authentication portion of the system is at least as strong as the encryption portion. Without that, the threat is really about hacking into the system rather than hacking the encryption process.

Let's take traditional ATA passwords as an example. In legacy computers, many individuals have depended on BIOS-level ATA security to protect their system. It can be easily demonstrated that many of the BIOSs in use today only support password lengths of up to 8 characters (or 64 bits). Further, these characters are often chosen as passwords that the user can remember, and therefore they are easy targets for amateur hackers.

With that understanding, some companies deploy fingerprint scanners to heighten the security of their systems. However, one needs to scrutinize the resolution and differentiation capabilities of the "signatures" that these scanners derive from the fingerprint images. A quick glance on the Internet shows scanner models with capabilities ranging from 30 to 100,000 enrollees. This translates to approximately 2^5 (5 bits) to 2^17 (17 bits). If you combine the best (17 bits) with a good 10-character randomly generated password (80 bits) you have a combined strength for your authentication password of 97 bits. Keep in mind that most BIOSs do not support this length of authentication key, and so this 97-bit authentication key will be reduced to some smaller number.

When considering the weakest link in the chain for systems that employ well-designed hard drive-based encryption, it is this authentication module that should be getting all the attention.

A few comparisons illustrate the superiority of hard drive-based encryption solutions over software-based encryption solutions:

- Key storage is accessible to the operating system with software encryption—which means it is open to attack. Hard drive encryption eliminates this vulnerability.
- Similarly, with software encryption the encryption process is observable in memory—again, not the case with hardware encryption.
- Software encryption can negatively impact system performance. There is no performance penalty with hardware encryption.

Summary of the Vulnerabilities of Software Encryption

	Hard Drive Encryption	Software Encryption
Key storage accessible to operating system (open to attack)	No	Yes
Encryption process observable in memory (open to snoop)	No	Yes
System performance negatively impacted by encryption process	No	Yes
User effort required to designate folders or files for encryption	No	Yes
Operating system upgrades more difficult than for a non-encrypted system	No	Yes

- With software encryption, the user specifies certain folders or files for encryption. With hardware encryption, everything written to the drive is encrypted, with no user intervention required.
- Operating system upgrades are more difficult for systems with software encryption than for non-encrypted systems. This is not the case for systems with hardware encryption solutions—they are no more difficult to upgrade than ordinary systems.

Further whitepapers are available if you would like more details on the above comparisons.

As cited in the examples above, software-based encryption has the traditional software threat exposures. This is not only true for the encryption engine but also for the authentication processes. To really button up a system, all of these software processes should be addressed well before the question of 128-bit versus 256-bit encryption is even a consideration.

As a final note, and segue to the encryption engine discussion, the following observation is made. Seagate Secure™ hard drives have been designed with authentication key size of 256-bits. So, while the drive is marketed as a 128-bit AES encrypting drive, the actual authentication key to unlock the drive supports a full 256 bits. That is the strongest level among all the commonly available encryption solutions.

Now that things are put into their proper perspective, let's dive into the encryption engine.

Encryption Engine

Why AES

There are three basic classes of NIST-approved cryptographic algorithms:

- To encrypt relatively short messages
- To compute digital signatures
- To establish or verify cryptographic keying material

Since the purpose of data-at-rest encryption is to transform data in a way that is fundamentally difficult to undo without knowledge of a secret key, symmetric key algorithms are deployed for FDE applications.

The NIST-approved algorithms for symmetric key algorithms are AES and TDES. The AES algorithm is specified in FIPS Pub 197[2]. AES encrypts and decrypts data in 128-bit blocks using 128-, 192- or 256-bit keys. NIST specifically states: "All three key sizes are considered adequate for Federal Government applications up through Classified Secret."

Triple DES (TDES) is defined in FIPS Pub 46-3. TDES encrypts and decrypts data in 64-bit blocks, using three 56-bit keys. Federal applications can use three distinct keys.

Extensive analysis by NIST (discussed in NIST Special Publication 800-57) found the AES algorithm to be stronger (i.e., the amount of work needed to "break the algorithm") than TDES, and that was one of the factors in its selection.

2 Federal Information Processing Standards Publications

128-Bit Versus 256-Bit AES Encryption

Practical business reasons why 128-bit solutions provide comprehensive security for every need

Choosing AES Key-Length

When implementing AES, Seagate had to decide which key strength to select. The selection process included the following considerations:

- NIST[1] has, in the reference document, concluded and recommended that all three key-lengths (128-bit, 192-bit and 256-bit) of AES provide adequate encryption until beyond calendar year 2031.
- NIST's recommendation above includes the threat model not only of predicting the key, but also of cracking the encryption algorithm. The difference between cracking AES-128 algorithm and AES-256 algorithm is considered minimal. Whatever breakthrough might crack 128-bit will probably also crack 256-bit.

Further, Seagate wanted to maximize the success of its solution by considering the additional business-side concerns:

- Must promote compliance with laws controlling export from the U.S. and import to other nations
- Must be cost-optimized
- Must be able to meet the needs of ALL target markets

AES-128 is sufficient or exceeds all the above criteria.

To put this in perspective, let's consider how big a number 128 bits really is. This represents 2 to the 128th power, or 3.4 x 10 to the 38th power (i.e., 38 zeros): 3,400,000,000,000,000,000,000,000,000,000,000,000.

If you assume:

- Every person on the planet owns 10 computers.
- There are 7 billion people on the planet.
- Each of these computers can test 1 billion key combinations per second.
- On average, you can crack the key after testing 50 percent of the possibilities.

Then (see calculation reference in Appendix):

- The earth's population can crack one encryption key (one drive only) in 77,000,000,000,000,000,000,000,000 years!
- In case you're wondering, cracking the second key/drive would take another 77,000,000,000,000,000,000,000,000 years.

The former was a rather simplified analysis. The European Network of Excellence in Cryptology performs a more sophisticated analysis regularly for the publication "Yearly Report on Algorithms and Keysizes." The most recent report, done January 2007, goes much deeper into analyzing the evolution of computing power (as a function of investment and technology evolution) and concludes in the following table:

Minimum Symmetric Key Size in Bits for Various Attackers

Attacker	Budget	Hardware	Minimum Security
"Hacker"	0 < $400 0	PC PC(s)/FPGA "Malware"	52 57 60
Small organization	$10K	PC(s)/FPGA	62
Medium organization	$300K	FPGA/ASIC	67
Large organization	$10M	FPGA/ASIC	77
Intelligence agency	$300M	ASIC	88

1 NIST (National Institute of Standards and Technology) is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all US government agency operations and assets. Standards for protecting US National Security Systems are specified by the National Security Agency (NSA).

While these key sizes are deemed acceptable for now, the other conclusion from the sources of the analysis is to add 14 bits to the key length to assure security for the next 20 years. That would result in a recommended key length of 102-bits (88 + 14) for top-level security for at least the next 20 years.

So why are solutions being marketed with 256-bit encryption? Marketing.

Bigger is perceived as better. It's as simple as that. Particularly when marketing a software solution, it is important to convey the perception of strength. It's a lot easier to add bits to the encryption algorithm than it is to tighten up all the holes in an open-system environment.

The reason 192-bit and 256-bit options were made available is because companies complained about TDES only being approved for one key length. NIST therefore evaluated three different key-length options for AES: 128, 192 and 256. Any of these key lengths will be implemented because they can be, rather than because of any specific needs. Top-secret military applications may demand 256-bit key-length because they can, and because it's available.

Other Important Considerations

When selecting an encryption system, there are solution-level factors that far outweigh any question about key length beyond 128 bits.

The following concerns must be satisfied in order to have complete, dependable data-at-rest protection:

- Are you enforcing sufficient password/ authentication credentials strength?
- Is your encryption system sufficiently hardened (processing in custom ASICs versus hackable software)?
- Is the communication path between the encryption module and the system/user-credentials secure?
- Has the candidate solution been approved by NSA?
- Can your solution be imported and exported to and from your target geographies?
- Does your solution provide adequate and secure key and password management services as demanded by centralized IT management organizations?
- Is your encryption solution architected in such a way that the keys never leave protected environments?

Seagate Secure drives provide the features and components to answer "yes" to all of these questions.

The following quote from the cited NIST publication offers a true perspective on the holistic approach for data security:

> The proper management of cryptographic keys is essential to the effective use of cryptography for security. Keys are analogous to the combination of a safe. If a safe combination becomes known to an adversary, the strongest safe provides no security against penetration. Similarly, poor key management may easily compromise strong algorithms. Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. All keys need to be protected against modification, and secret and private keys need to be protected against unauthorized disclosure. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys.
>
> Users and developers are presented with many choices in their use of cryptographic mechanisms. Inappropriate choices may result in an illusion of security, but little or no real security for the protocol or application. This recommendation (i.e., SP 800-57) provides background information and establishes frameworks to support appropriate decisions when selecting and using cryptographic mechanisms.

128-Bit Versus 256-Bit AES Encryption

Practical business reasons why 128-bit solutions provide comprehensive security for every need

Summary

- 128-bit hard drive-based encryption is clearly sufficient to address all commercial and non-top secret government applications.
- Once the encryption engine discussion is put to rest, much more energy should be focused on solution-level deployment issues.
- The vulnerabilities for data leakage are not a result of encryption key size when 128-bit keys are deployed. The primary vulnerabilities are in software, key storage and authentication.
- When these areas are properly addressed, the data protection solution that deploys 128-bit AES encryption provides comprehensive security for every need.

Appendix

Computation Reference for 128-Bit Key Crack Example	
People	7.00E+09
Computers per person	10.00
Computers	1.00E+09
Combos per second per computer	7.00E+19
Total combos per second	7.00E+19
Seconds per year	3.15E+07
Total combos per year	2.22E+12
128-bit key combos (*50%)	1.70E+38
Years to crack	7.66E+25

Publication References

NIST (National Institute of Standards and Technology) Special Publication 800-57 (May 2006)
http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf

(D.SPA.21ECRYPT Yearly Report on Algorithms and Keysizes) by the European Network of Excellence in Cryptology (January 2007)
http://www.ecrypt.eu.org/documents/D.SPA.21-1.1.pdf

http://www.crypto.com/papers/keylength.pdf

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIA/PACIFIC Seagate Technology International Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 130–136, rue de Silly, 92773, Boulogne-Billancourt Cedex, France 33 1-4186 10 00