CSD 451: Applied Cryptography

Group 3: DISK ENCRYPTION

Ashish Kharbanda - 1910110098, Jyothis Mahadev G - 1910110183, Samarth Gupta - 1910110338

Introduction

Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. It is used to prevent unauthorized access to data storage.

Our Idea

We are implementing a software based encryption algorithm which will encrypt the whole drive. The application will be implemented in Linux and will perform disk encryption using The AES algorithm. We are planning to use C++ to code our backend, and develop a frontend in Linux.

However, we are planning on making our programme independent of the operating system because it is built on a software-based encryption system that uses the AES encryption technology, which can be deciphered regardless of the operating system.

Advanced Encryption Standard (AES)

It is a specification for the encryption of electronic data. AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES uses keys of 192 and 256 bits for heavy-duty encryption purposes. It is the algorithm trusted as the standard by the U.S. Government and numerous organizations.

AES data encryption is a more mathematically efficient and elegant cryptographic algorithm, but its main strength rests in the option for various key lengths, making it exponentially stronger than the 56-bit key of DES. Other encryption algorithms.

Other Encryption Algorithms

Triple DES (Triple Data Encryption Algorithm)

It is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. It is based on DES, which is an adapted version of DES. Triple DES uses three individual keys with 56 bits each.

RSA Algorithm

It's an asymmetric algorithm i.e. works on two different keys, public key and private key. Uses public keys of 1024, 2048, or 4096 bits in length, which is a product of multiplying two huge prime numbers together.

Blowfish

This symmetric cipher i.e it uses the same key for encryption and decryption, splits messages into blocks of 64 bits and encrypts them individually.

Twofish

It is also a symmetric key block cipher. Keys used in this algorithm may be up to 256 bits in length.

Paramet ers\Algo rithm	AES	DES	3DES	BLO WFIS H	TWO FISH
Key Length	128,192 or 256 bits	56 bits	112 and 168 bits (interna lly)	32 to 448 bits	128 bits 192 bits 256 bits
Cipher type	Symmetri c block cipher	Symm etric block cipher	Symme tric block cipher	Symm etric block cipher	128 bits
Block size	128,192 or 256 bits	64 bits	64 bits	64 bits	128 bits
Keys	1	1	3	Public	Public
Possible keys	2^{128},2^{192} or 2^{256}	2^{56}	2^{112} or 2^{168}	2^{32} or 2^{448}	256
Attacks prone to		Differ ential and linear crypt analys is	Differe ntial, brute force attack	Differ ential, brute force attack	Highl y secure with still no crypta nalysi s found

Implementation

Disk encryption is possible with a variety of solutions available on the market. However, they differ significantly in terms of features and security. Software-based, hardware-based within the storage device, and hardware-based elsewhere are the three basic categories (such as CPU or host bus adapter). Self-encrypting drives use hardware-based full disk encryption within the storage device and have no performance impact. Furthermore, the media-encryption key never leaves the device and is thus unavailable to any operating-system virus.

The Opal Storage Specification from the Trusted Computing Group is an industry standard for self-encrypting drives. Although CPU versions may still have an impact on performance, external hardware is significantly faster than software-based alternatives, and the media encryption keys are not as well protected. Now because symmetric cryptography is usually strong, the authentication credentials are usually a big potential flaw in all circumstances.

OS dependent implementation / differences

General- purpose file system with encryption

- AdvFS on Digital Tru64 UNIX
- Novell Storage Services on Novell NetWare and Linux
- NTFS with Encrypting File System (EFS) for Microsoft Windows
- ZFS since Pool Version 30
- Ext4, added in Linux kernel on June 2015
- F2FS, added in Linux
- APFS, macOS High Sierra (10.13) and later.

Name	Windows NT	Windows Mobile (incl.Pocket PC)	FreeBSD	Linux	Mac OS X	NetBSD	OpenBSD	DragonFly BSD	Android	iOS
Aloaha Crypt Disk	Yes	No	No	No	No	No	No	No	?	?
BestCrypt Volume Encryption	Yes	No	No	No[42]	Yes	No	No	No	?	?
BitArmor DataControl	Yes	No	No	No	No	No	No	No	?	?
BitLocker	Yes	No	No	Partial[43]	Partial[43]	No	No	No	No	?
Bloombase StoreSafe	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	?	?
Boxcryptor	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes
CenterTools DriveLock	Yes	No	No	No	No	No	No	No	?	?
CGD	No	No	No	No	No	Yes	No	No	?	?
Check Point Full Disk Encryption	Yes	Yes	No	Yes[44]	Yes	No	No	No	?	?
CipherShed	Yes	No	No[45]	Yes	Yes	No	No	No	Yes[46]	?
CrossCrypt	Yes[47]	No	No	No	No	No	No	No	No	?
CryFS	Yes	No	Yes	Yes	Yes	Yes	No	Yes	No	?
Cryhod	Yes	No	No	Yes	No	No	No	No	?	?
Cryptainer	Yes	Yes[48]	No	No	No	No	No	No	?	?
CryptArchiver	Yes	No	No	No	No	No	No	No	?	?
Cryptic Disk	Yes	No	No	No	No	No	No	No	No	No
Cryptoloop	Yes[49]	No	No	Yes	No	No	No	No	?	?
Cryptomator	Yes[50]	No	No	Yes	Yes	No	No	No	Yes	Yes
CryptoPro Secure Disk Enterprise	Yes	No	No	No	No	No	No	No	No	?
CryptoPro Secure Disk for BitLocker	Yes	No	No	No	No	No	No	No	No	?
Cryptsetup / Dmsetup	Yes[49]	No	No	Yes	No	No	No	Yes	?	?
CryptSync	Yes	No	No	Yes	Yes	No	No	No	No	?
Discryptor	No	No	No	No	No	No	No	No	?	?
DiskCryptor	Yes	No	No	No	No	No	No	No	?	?
DISK Protect	Yes	No	No	No	No	No	No	No	?	?
Dm-crypt / LUKS	Yes[49]	Yes[51]	No	Yes	No	No	No	Yes	?	?
DriveCrypt	Yes	No	No	No	No	No	No	No	?	?
DriveSentry GoAnywhere 2	Yes	No	No	No	No	No	No	No	?	?
E4M	Yes	No	No	No	No	No	No	No	?	?
e-Capsule Private Safe	Yes	No	No	No	No	No	No	No	?	?
eCryptfs	No	No	No	Yes	No	No	No	No	?	?
EgoSecure HDD Encryption	Yes	No	No	No	No	No	No	No	?	?
EncFS	Yes[52]	Yes[53]	Yes (FUSE)	Yes (FUSE)	Yes[52]	Yes (FUSE)	Yes (FUSE)	Yes (FUSE)	Yes[53]	?
EncryptStick	Yes	No	No	Yes	Yes	No	No	No	?	?
EncryptUSB	Yes	No	No	No	Yes	No	No	No	?	?
FileVault	No	No	No	No	Yes	No	No	No	?	?
FileVault 2	No	No	No	Partial[54]	Yes	No	No	No	?	?
FREE CompuSec	Yes	No	No	No	No	No	No	No	?	?

Hashing (To be done)

AES-hash is a secure hash function that accepts any bit string as input and outputs a fixed length (in this example, 256 bit) text.

Any changes to the input should cause the output to become completely jumbled. Finding two files that hash to the same value should take about 2128 operations on average. On average, 2255 operations should be required to locate a file that hashes to a certain value. It should be impossible to deduce anything about a file from its hash in a way that is faster than guessing at the original file.

AES-hash parallelizes to the extent that key setups and encryptions can be done in parallel, but a file must be hashed serially as a whole. However, it just requires a single pass. Secure hash modes don't require any keying material, but keyed variants are simple to create.

AES-hash requires a small fixed amount of memory to store its Hi values, but only a single block of the hashed file should be kept in memory at any given time.AES-hash works with arbitrary bit strings, allowing it to be used in a wide range of applications.

Secure hash functions all work as a perverse compression method, reducing everything to a small fixed size, in this case 256 bits.

Attacks on AES

Side-channel attacks are a significant threat to AES encryption. Rather than attempting a brute-force attack, side-channel attacks seek out information that has been leaked from the system. Side-channel attacks, on the other hand, may lower the amount of potential combinations required to brute-force attack AES.

Side-channel attacks include gathering information about a computer device's cryptographic processes and using that information to reverse-engineer the device's cryptography system. Timing information, such as how long it takes the computer to perform computations; electromagnetic leaks; audio clues; and optical information, such as from a high-resolution camera, may all be used in these attacks to uncover additional information about how the system is processing the AES encryption. By closely monitoring the cipher's shared use of the processors' cache tables, a side-channel attack was successfully utilized to extract AES-128 encryption secrets in one example.

Side-channel attacks can be avoided by preventing data from escaping in the first instance. Furthermore, using randomization techniques can help erase any link between the cipher-protected data and any leaked data that could be collected via a side-channel attack.

Resources

- https://en.wikipedia.org/wiki/Disk_encryption
- https://blog.storagecraft.com/5-common-encryption-algorithms/
- https://en.wikipedia.org/wiki/Disk_encryption#cite_note-ColdBoot-5
- https://www.researchgate.net/publication/334724160_A_Comparative_Study_and_Analysis_of_Cryptographic_Algorithms_RSA_DES_AES_BLOWFISH_3-DES_and_TWOFISH
- https://www.encryptionconsulting.com/education-center/what-is-twofish/
- https://www.embedded.com/encrypting-data-with-the-blowfish-algorithm/
- https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

- https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
- https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software