Application

Description automatically generated

Analysis of the NTFS file system for Windows 11 in a security context

# High level description of NTFS security features

Released in 1993 for Windows NT 3.1, NTFS (New Technology File System) replaced FAT as the default file system on Windows (Custer, 1994). As a modern file system, NTFS places a large importance on security.

Some examples of NTFS security features are:

* Access control lists (ACLs)
  + ACLs are a way of restricting access to files and directories on a network or computer to certain specified users and/or groups at different levels of access (Microsoft, 2022).
* Encrypting File System (EFS)
  + EFS is a NTFS feature that allows a user to encrypt individual files and directories of their choosing. An EFS encrypted file or directory can only be opened by the user (Microsoft, 2023).
* BitLocker
  + BitLocker is a full drive encryption solution for the NTFS file system. BitLocker will prevent the OS (Operating System) from being unencrypted until a pre-defined PIN is provided (Microsoft, 2022).

Timeline

Description automatically generated with low confidence

Figure Timeline showing Windows releases and when features were introduced **(NOTE: for brevity this does not include all Windows releases)** (Russinovich, 2006) (Dubrawsky, 2003) (Microsoft, 2005)

# Detailed description of how Windows supports and provides the listed security features

## ACLs

Both users and groups (referred to as security principals) can be defined and are represented by a unique SID (Security identifier). An administrator can then add security principals and assign read, write, modify, or full control permissions for files and directories. Sub-folders of a folder with an access control list will inherit permissions (Microsoft, 2022). ACL meta-data is stored in the master file table (MFT) (Microsoft, 2021)

## EFS

To encrypt files, EFS uses a combination of a public and a private key – known as “asymmetric encryption”. When a file is encrypted with EFS, a unique File Encryption Key (FEK) is generated. The FEK is used to encrypt the contents of the file in blocks. The FEK is stored in a header of the encrypted file and is then encrypted with a public key taken from the user’s certificate from the user profile (Microsoft, 2012). The public key is stored in the computer’s certificate store which is located in the computer’s registry (Microsoft, 2021)(Microsoft, 2012).

Diagram

Description automatically generated

Figure 2 diagram showing the structure of a file encrypted with EFS (Microsoft, 2012)

As shown in the diagram above, “recovery agents” can be created. This is in the event that the private key is damaged or lost. The local or domain administrator will automatically be assigned as recovery agents. Private keys will be created for each agent and can be decrypted with the public keys (Microsoft, 2012). Recovery agents can also be manually created (Microsoft, 2022).

EFS uses transparent encryption, this means that when an authorized user opens the folder the user certificate public key is automatically used to decrypt the private key and decrypt the contents as plaintext. From an authorized user’s perspective, the decryption is seamless (Microsoft, 2012).

There are four different services that EFS uses to encrypt files: CryptoAPI, EFS Service, EFS Driver, and EFS FSRTL (EFS File System Run-Time Library). EFS service uses CryptoAPI to generate the FEK and public key and then creates the header for the encrypted file. EFS driver communicates with EFS service to request key management service from CryptoAPI for encryption and decryption which is then passed to EFS FSRTL to perform file system operations (open, read, write, and append) (Microsoft, 2012).

Diagram

Description automatically generated

Figure 3 diagram to show full operation of EFS (Microsoft, 2012)

## BitLocker

It is recommended that BitLocker is enabled in conjunction with a TPM (Trusted Platform Module) chip. However, BitLocker can be used to encrypt a NTFS drive without a TPM, but this requires that a USB startup key to be inserted into the computer on startup (Microsoft, 2022). The TPM chip is used by BitLocker to create and store cryptographic keys (Microsoft, 2023)

When BitLocker is installed, an unencrypted system partition is automatically created and is used to boot, decrypt, and load the OS (Microsoft, 2022). For encryption, BitLocker uses AES (Advanced Encryption Standard) with a default key length of 128 bits – this can be changed to 256 bits through group policy (Microsoft, 2022). When data is read from a BitLocker protected drive, sectors are only decrypted as they are requested from system read operations (Microsoft, 2022).

Raw data is encrypted with a full volume encryption key, this is then encrypted with a volume master key. Finally, the volume master key is also encrypted. These keys are stored in the encrypted drive (Microsoft, 2022)

To reduce encryption time, BitLocker can be configured to use “used disk space only encryption” and only encrypt areas of the disk that contain data (Microsoft, 2022). BitLocker can also be configured to only startup after a USB startup key is inserted (Microsoft, 2022). In the event that the drive cannot be unlocked normally, there are three ways of recovering data encrypted using BitLocker:

* Recovery passwords can be stored on a USB drive or accessed through an associated Microsoft account. Note: recovery passwords are only stored on a Microsoft account if the associated PC is a member of a domain. (Microsoft, 2022)
* Data recovery agents can be set-up and enter their credentials to unlock the drive. (Microsoft, 2022)
* BitLocker can be setup to store the recovery password in ADDS (Active Directory Domain Services). An administrator can then access the recovery password from ADDS. (Microsoft, 2022)

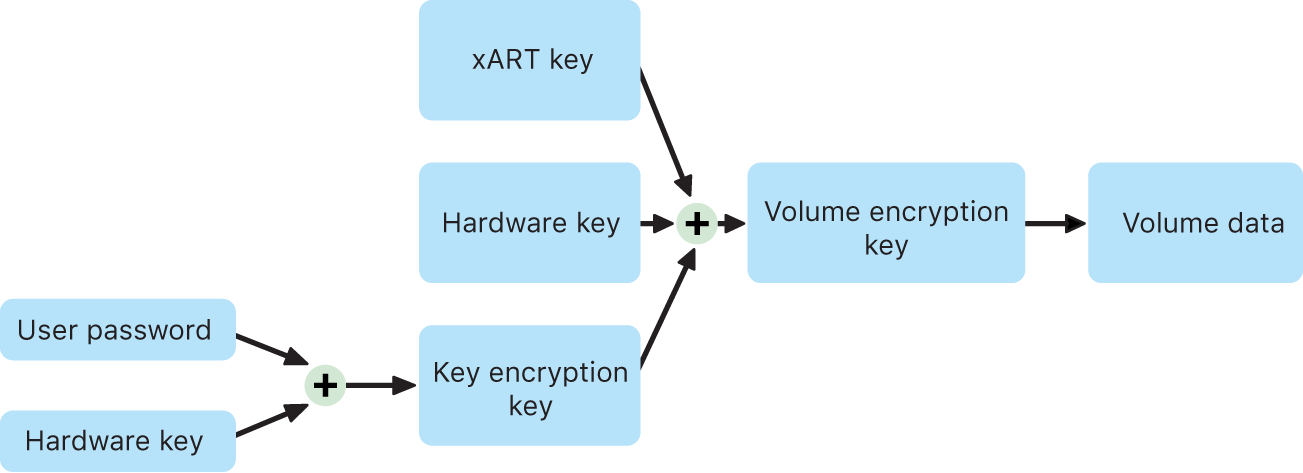
# A comparison of NTFS security features compared to APFS

MacOS Ventura uses the filesystem APFS (Apple File System) (Apple, 2023)

## BitLocker Vs. FileVault 2

APFS offers a similar full-disk encryption service to BitLocker known as FileVault 2. FileVault 2 uses the AES-XTS encryption algorithm compared to AES-128 that BitLocker uses. Unlike BitLocker the encryption algorithm is not configurable. (Apple, 2022) Similar to how BitLocker uses the TPM, File Vault utilizes a specialized secure subsystem called the “secure enclave processor (SEP)”. Unlike BitLocker (which stores keys in an encrypted partition), Both encryption key storage and any encryption processing occurs in the SEP (Apple, 2021) (Apple, 2022). FileVault also offers recovery in the form of a “recovery key” (Apple, 2023)

Key management in FileVault 2 is slightly more complex than in BitLocker and is shown in the diagram below



demonstrates the key management in FileVault 2 (Apple, 2022)

## EFS Vs. APFS encrypted containers

APFS offers similar utility to EFS. Users can create encrypted disk images that serve as secure containers. Either 128-AES or 256-AES encryption can be used. Files in the container are encrypted and decrypted in real-time (Apple, 2022)

## Windows ACLs Vs. MacOS ACLs

ACLs exist in APFS and are practically identical to NTFS ACLs. Similar to NTFS ACLs, both individual users and groups of users can be assigned individual permissions. However, the privilege options are less extensive with only “read & write” and “read only” being available (Apple, 2023). APFS ACLs also use ID for groups and users to verify that they can access the file (Apple, 2020)

# Effects that listed security features have on application developers

## ACLs

Developers will have to ensure that certain precautions are put in place to maintain ACLs if the program they are developing transfers files. For example, Microsoft detail specific code that a developer should use to ensure that ACL meta-data is preserved in Azure (Microsoft, 2023).

## EFS

Transactional NTFS (TxF) is a Windows feature that allows developers to safely update and manipulate files. TxF achieves this by creating a restore point for a file before any updates and then processing the update. If the update fails then the file can simply be restored from the restore point, otherwise it is committed (Microsoft, 2021). Any file encrypted with EFS cannot be processed with TxF, and TxF cannot encrypt a file (Microsoft, 2021).

SQL (Structured Query Language) database files can interact poorly with EFS; specifically, the “read ahead” and “checkpoint” features. This is due to how “asynchronous I/O requests from SQL Server are converted to synchronous I/O operations on an EFS-encrypted database file”. Microsoft recommends that if a developer requires that SQL database files be encrypted they should use an alternative encryption service (Microsoft, 2022).

## BitLocker

If the program that is being developed alters the master boot record (MBR) a developer must be extremely careful to ensure that any changes work within BitLocker security requirements and do not alter the security environment too drastically. Otherwise, once changes are made, the computer might boot up in recovery mode or fail to boot entirely (Microsoft, 2022)

# Conclusion

One interesting feature I found in my comparison of APFS security features was that consistently all cryptographic processing and key storage was done in the SEP. However, although the NTFS features I investigated made use of a similar cryptographic processor (the TPM), encryption keys are not stored in the TPM but stored either in registers (for EFS) and in an encrypted volume on the hard drive for BitLocker.

In the case of EFS, if an attacker was able to login to the computer; it seems feasible to me that they could gain access to the encryption keys and circumvent EFS on another computer. A dedicated secure storage component for encryption keys would add a lot more security.

**[write about** [**this**](https://csrc.nist.gov/publications/detail/sp/800-38e/final)**]**

# Appendix

BitLocker was originally known as “Secure Startup”