NTFS (New Technology File System) is the default file system of modern Windows, including Windows 10. It provides several security features (Microsoft, 2021a). Privileging, determining which users or groups can access or modify files or folders. Auditing, which logs access and changes to files or folders. Security Descriptors, consisting of user access identifiers for Access Control Lists, and control lists for accessing and auditing policies. Additionally, Security Descriptors allow file permissions to be defined. Files within the NTFS file system are also individually encrypted using the Encrypted File System, or EFS (Microsoft, 2023a).

Privileging is used in conjunction with the User Right’s found within Access Control Lists (Microsoft, 2023b). Privileges are held by a caller (Microsoft, 2023c). Privileges dictate system-level permissions of users and groups, such as the ability to modify any file even in cases where File Permissions may not permit such. Consequently, they are closely tied to the File System and provide an additional layer of security. Privileging was introduced alongside Access Control Lists in Windows NT 3.1 with NTFS in 1993. Earlier file systems, such as FAT (File Allocation Table) did not include privileging (Microsoft, 2008).

Auditing works in conjunction with security descriptors. If auditing is enabled for an object or event, then the security descriptor for the file will include an SACL (System Access Control List) (Microsoft, 2009a). This informs which actions should be audited. When an action that should be audited occurs, then a record is created in the Security-category of Window’s Event Viewer. This record includes information about the user, action preformed, and time occurred. Administrators may specify which objects are audited, including by whom and which user-class, as well recording of the permissions that led to that to that event being generated (Microsoft, 2022). Auditing was introduced apart of Windows NT 3.1 which released in 1993. The capabilities were enhanced in subsequent releases, with Windows NT 3.5 and Windows NT 4.0.

Security Descriptors are a critical component of security in the NTFS. They are a data structure that contains information about the security of an object (Microsoft, 2021b). They’re informed by Access Control Entries (ACEs) which Access Control Lists (ACLs) are made of. Security Descriptors are composed of three pieces of information (Microsoft, 2021c). First, a security identifier which determines the owner of an object, such as a user or group. Second, a Discretionary Access Control List (DACLs) which defines a user or group’s access rights to an object, including level of access and basic file permissions; read, write, execute (Microsoft, 2021d). Third, a System Access Control List (SACLs) which specifies audit policy including which users or groups should be audited upon an attempt to access the object (Microsoft, 2021c). Security Descriptors also support inheritance. Child folders inherit permissions of the parent, with design in place to prevent security vulnerabilities from such (Microsoft, 2023d). Permissions will not be updated upon folder move for instance. Security Descriptors were implemented in Windows NT 3.1 with NTFS in 1993.

Encrypted File System (EFS) is a feature of NTFS that provides encryption of files or folder content. EFS uses a public-key system (Microsoft, 2023a). Files are encrypted with a randomly generated symmetric key (Microsoft, 2023e). This key is then encrypted with the user’s public-key. User’s must provide their matching private key to decrypt files to allow access. EFS uses AES-256 algorithm for encryption of a file’s data (Microsoft, 2023f). EFS was implemented into NTFS version 3.0 with the release of Windows 2000 (Microsoft, 2009b).

APFS (Apple File System) is the default file system of macOS. It provides several security features which are comparable to those found on Windows’ NTFS.

Encryption can be preformed on APFS at the file system level (Apple, 2020). Consequently, APFS encryption is integrated into the Operating System at a lower level than Windows’ EFS which is a system driver (Microsoft, 2023a). In terms of algorithms, APFS uses AES-XTS whereas EFS uses AES (Apple, 2020). Encryption keys on APFS are stored within the device on a component called the ‘Secure Enclave’ which maintains sensitive information separate from the CPU (Apple, 2021). In comparison, EFS’ encryption keys are stored within user data (Microsoft, 2023a). Unlike EFS’ public-private keys, APFS’ are solely symmetric (Apple, 2020). APFS also encrypts per-volume (per storage-drive) whilst EFS encrypts per-file.

APFS may alternatively be encrypted through FileVault, which encrypts the entire startup disk on a MacOS whereas APFS’ native encryption does so per-volume. Implementation differs such as how FileVault stores keys on the startup disk itself and uses AES-XTS-128 (Apple, n.d; 2022).

Access Rights on APFS