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

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)
* Encrypting File System (EFS)
* BitLocker

ACLs (introduced in Windows NT 3.51 (Russinovich, 2006)) are a way of restricting access to system objects on a network or computer. 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 specific objects such as files, folders, printers, and registry keys. Sub-folders of a folder with an access control list will inherit permissions (Microsoft, 2022)

EFS (introduced in 2000 in NTFS 3.0 alongside Windows 2000) allows a user to encrypt individual files and directories of their choosing (Microsoft, 2023). To encrypt files, EFS uses a combination of 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)

Diagram

Description automatically generated

Figure 1 diagram showing the structure of a file encrypted with EFS (Microsoft, 2012)