

Flipped Classroom Session 6: Data Encryption

CS-E3130 Information Security, 28.09.2023

1. Encrypted filesystem

1. Explain an advantage of file-level encryption compared with full-disk encryption.
2. How vulnerable (or not) is the Windows Encrypted Filesystem to brute-force attack?

2. Full-disk encryption

1. Explain an advantage of full-disk encryption compared with file-level encryption.
2. Bitlocker can use a Trusted Platform Module (TPM) to protect disk encryption keys. What advantages does the TPM provide over a software-only solution?
3. Suppose you gain physical access to a powered-off desktop machine whose hard disk is protected with BitLocker. How can you access data stored on the machine? State your assumptions.