Class Activity

Title: Disk Encryption using VeraCrypt

Overview

The aim of this class activity is to familiarize students with practical aspects of disk encryption, enhancing their understanding of data security measures. Students will gain hands-on experience by encrypting a disk using two different tools: VeraCrypt for any Windows system and BitLocker for Windows 10. This exercise will help students learn how to secure sensitive data effectively and understand the operational characteristics of both encryption tools.

⚠️ ONLY DO THIS EXERCISE IN A VIRTUAL MACHINE. DO NOT DO THIS ON YOUR MAIN COMPUTER.⚠️

Learning Objectives

- Understand the fundamental principles and importance of disk encryption.
- Learn to set up and configure disk encryption using VeraCrypt.
- Learn to enable and configure BitLocker encryption on Windows 10.
- Develop an awareness of the security features and considerations associated with encrypting and accessing encrypted data.

Instructions:

Part 1: Using VeraCrypt for Disk Encryption

VeraCrypt is a free, open-source disk encryption software that can encrypt an entire partition or storage device. Here is how to use it:

1. **Download and Install VeraCrypt**:
    - Go to the VeraCrypt website and download the latest version of VeraCrypt.
    - Install the software by following the on-screen instructions.
2. **Launch VeraCrypt**:
    - After installation, open VeraCrypt from your Start menu.
3. **Create a Volume**:
    - Click on ‘Create Volume’ to start the VeraCrypt Volume Creation Wizard.
    - Choose ‘Encrypt a non-system partition/drive’ and click ‘Next’.
4. **Volume Type**:
    - Select ‘Standard VeraCrypt volume’. (You can also create a hidden volume for additional security.)
5. **Select Device**:
    - Click on ‘Select Device’ and choose the partition or external drive you want to encrypt.
6. **Encryption Options**:

- Choose an encryption algorithm. VeraCrypt offers several options like AES, Serpent, and Twofish. AES is typically recommended for its balance of speed and security.
- Select a hash algorithm, such as SHA-512.

7. **Volume Password**:
   - Set a strong password that will be used to encrypt the volume. Make sure it is complex and secure.
8. **Format Options**:
   - Choose the filesystem you wish to use (like FAT, exFAT, or NTFS) and then click ‘Format’ to start the encryption process.
   - This step may take a significant amount of time, depending on the size of the drive and the speed of your computer.
9. **Mount and Use Your Encrypted Volume**:
   - Once the drive is encrypted, go back to the main VeraCrypt window, select a drive letter, and click on ‘Select Device’ to choose your encrypted volume.
   - Click ‘Mount’, enter your password, and access your securely encrypted drive.

Part 2: Using BitLocker on Windows 10 - ONLY DO THIS EXERCISE IN A VIRTUAL MACHINE. DO NOT DO THIS ON YOUR MAIN COMPUTER.

BitLocker is a built-in encryption feature in Windows 10 Pro, Enterprise, and Education editions.

1. **Enable BitLocker**:
    - Open Virtual Box and load your Windows 10 virtual MachineOpen the Control Panel, go to ‘System and Security’, then click on ‘BitLocker Drive Encryption’.
    - Choose the drive you want to encrypt and click ‘Turn on BitLocker’.
2. **Choose How to Unlock the Drive**:
    - You can choose to unlock the drive at startup with a password or a smart card. Select ‘Use a password to unlock the drive’ and enter a strong password.
3. **Save Recovery Key**:
    - BitLocker will prompt you to save a recovery key, which can be used to access your data if you forget your password. Save the recovery key to your Microsoft account, a USB drive, a file, or print it.
4. **Encrypt the Whole Drive**:
    - Select ‘Encrypt entire drive’. This is more secure and is recommended if the drive has been used before.
5. **Choose Encryption Mode**:
    - For a new drive, use ‘New encryption mode’. For drives used in older versions of Windows, select ‘Compatible mode’.
6. **Start the Encryption Process**:
    - Click ‘Start encrypting’. The encryption process will begin, and the duration will depend on the size of the drive. You can still use your PC during this time, but performance might be slower.
7. **Check Encryption Status**:
    - You can check the progress by going back to the ‘BitLocker Drive Encryption’ menu in Control Panel.

Submission

Document your work and upload the document in Google Classroom.