RANSOMWARE ATTACKS

COMPUTER NETWORKING

Time: 60 mins

Introduction

In this class, the student/s will learn how to lock the files, encrypt and decrypt the files using the Fernet key.

New Commands Introduced

● from cryptography.fernet import Fernet	Directs to the fernet module from cryptography Imports the Fernet module
● Fernet.generate_key()	Generates a key value using the Fernet module
● encryptedKey.write(key)	Stores the key value using write method in the encryptedKey.key file
● Fernet(key).encrypt(rawData)	Encrypts the data and locks using encrypted Fernet key

Vocabulary

- The **fernet module** of the cryptography package has inbuilt functions for the generation of the key, encryption of plaintext into ciphertext, and decryption of ciphertext into plaintext using the encrypt and decrypt methods respectively.
- A **fernet key** is used to encrypt and decrypt fernet tokens.
- **Ransomware** is the attack performed by installing an application from unprotected sources or clicking on a link which shares a virus.

Learning Objectives

Student/s should be able to:

- ***Recall*** the encryption and decryption using the cryptography method.
- ***Demonstrate*** the generation of Fernet key which can be used to perform a ransomware attack on files.
- ***Explain*** how files are encrypted and decrypted using the Fernet key.

Activities

Class Narrative: *(3 mins)*

- Brief the student/s that sometimes opening a file gives error and can throw a notification to inform on cybersecurity attack.

Concept Introduction Activity: *(4 mins)*

- Let the student/s observe that the files are locked with an encryption key and a text file is shared to inform and trade for the attack performed.
- Explain how ransomware attacks are performed, different sources of ransomware and its kinds.
- Using the slides, explain that the student/s will learn:
    - to generate an encryption key
    - to encrypt the file data
    - to decrypt the file data

Activity 1: Generate an Encryption Key *(16 mins)*

Teacher Activity: *(8 mins)*

- Recall we used cryptography to perform asymmetric encryption and decryption using a public and private key.
- Introduce the Fernet module used in cryptography for encryption and decryption and how fernet key can be generated.
- Demonstrate how to generate the fernet key and store it using the write mode method.

Student Activity: *(8 mins)*

- Guide the student/s to generate an encryption key using the Fernet module.

Activity 2: Encrypt the File Data *(10 mins)*

- Explain how we will open a file, read its data and encrypt it.
- Explain how we will write the encrypted data to another file.

Student Activity: *(10 mins)*

- Guide the student/s to encrypt the file data using the fernet key.

Activity 3: Decrypt the File Data *(12 mins)*

- Explain how you can either use a secret password or the encrypted key to unlock the encrypted files.
- Explain how using an encrypted key, we need to decrypt the fernet key to unlock the file and then decrypt the file data.

Student Activity: *(6 mins)*

- Guide the students to decrypt the file data using the fernet key.

Introduce the Post class project: *(2 min)*

- Encrypt and decrypt the file data by asking an input form the user.

Test and Summarize the class learnings: *(5 mins)*

- Check for understanding through quizzes and summarize learning after respective activities.
- Summarize the overall class learning towards the end of the class.

Additional activities:

- Encourage the student/s to add the functionality to not create a key if a Fernet key is already created such that file can be decrypted without an error.
- Encourage the student/s to encrypt the file only if the file cannot be decrypted with the saved Fernet key.

State the Next Class Objective: *(1 min)*

- In the next class, student/s will learn about the IDOR attacks in cybersecurity.

U.S. Standards:

CSTA: 2-AP-11, 2-AP-12, 2-AP-13, 2-AP-14, 2-AP-19

Links Table		
Activity	Activity Name	Link
Class Presentation	RANSOMWARE ATTACKS	https://s3-whjr-curriculum-uploads.whjr.online/de76152a-a094-4bfd-ae74-a766145b7392.html
Explore Activity	RANSOMWARE ATTACKS	https://s3.amazonaws.com/media-p.slid.es/uploads/2071954/images/10989645/Slide_4-1.gif
Teacher Activity 1	Generate an Encryption Key	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-TAS-BP
Teacher Reference: Teacher Activity 1 Solution	Generate an Encryption Key	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-TAS

Student Activity 1	Generate an Encryption Key	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS-BP
Teacher Reference: Student Activity 1 Solution	Generate an Encryption Key	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS
Teacher Activity 2	Encrypt the File Data	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-TAS-BP
Teacher Reference: Teacher Activity 2 Solution	Encrypt the File Data	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-TAS
Student Activity 2	Encrypt the File Data	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS-BP
Teacher Reference: Student Activity 2 Solution	Encrypt the File Data	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS
Teacher Activity 3	Decrypt the File Data	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-TAS-BP
Teacher Reference: Teacher Activity 3 Solution	Decrypt the File Data	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-TAS
Student Activity 3	Decrypt the File Data	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS-BP
Teacher Reference: Student Activity 3 Solution	Decrypt the File Data	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS
Student's Additional Activity 1	Create a Single Fernet Key	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS-BP
Teacher Reference: Student's Additional Activity 1 Solution	Create a Single Fernet Key	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS
Student's Additional Activity 2	Encrypt the File Once	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS-BP
Teacher Reference: Student's Additional Activity 2 Solution	Encrypt the File Once	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-SAS
Post Class Project	Perform Crypto-ransomware Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-PCP-BP
Teacher Reference: Post Class Project Solution	Perform Crypto-ransomware Attack	https://github.com/Tynker-Computer-Networks/TNK-M16-C125-PCP